

Neutrality and Cyberspace



Marcel Sebastian Stolz
Collegium Magnae Aulae Universitatis Oxon
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy

Michaelmas 2022

To my grandparents
Dr. Jaromír and Jarmila Hladký
Who taught me the value of freedom.

To my family and friends
For their support in challenging times.

Acknowledgements

First of all, I would like to express my gratitude to my supervisors, Prof Michael Goldsmith and Dr Lucas Kello. Both have always taken great interest in my unconventional topic and have provided support and input when needed.

Michael was particularly helpful in keeping up my morale during very challenging times; he always added the required pinch of humour, occasional motivational breakfasts, as well as any solid or liquid nutrition when a day had to be lightened up. I would particularly like to thank him for providing relief from sorrow at his French mansion.

Lucas was very supportive by welcoming me to a discipline that I had no academic background in; I have excellent memories of a fascinating introduction to the questions of *international relations with respect to cyberspace* during my first year in Oxford.

Both of my supervisors have been tremendously helpful in bridging the gap between academic disciplines: They always reassured me that my topic was highly relevant whenever I was in doubt.

Next, I would like to thank the foundations that supported me financially and through education along the path of my DPhil. I was fortunate enough to receive a stipend for the living costs during my “CDT year” from the *Hasler Stiftung*¹ in Bern, Switzerland. Thereafter, I was admitted into the glorious ranks of Germany’s *Konrad Adenauer Stiftung*² (“KAS”) as a graduate scholar. Its many seminars widened my horizon and I enjoy many good moments within the community of academics and scholars; the local group of KAS scholars in Oxford provided a home through its very friendly environment, and the financial support by means of the scholarship enabled me to pursue my doctoral degree. Janggen-Pöhn-Stiftung³,

¹See <https://haslerstiftung.ch/>

²See <https://www.kas.de/de/home>

³See <http://www.janggen-poehn.ch/>

based in St Gallen (Switzerland) provided some funds for my studies when my living costs were not covered through other scholarships. The UK's EPSRC covered my course fees in Oxford and provided grants for my conference travels, which equally deserves my gratitude.

I would also like to thank my assessors and examiners, Prof William H. Dutton, Dr Robert Johnson, and Prof Johannes M. Bauer, who have provided valuable feedback to my work along the formal assessment and examination process.

My research group was an excellent home during my time in Oxford, and many pub lunches, excursions, and walks have offered a great distraction from work that enabled me to refuel my energy levels and free up some headspace for research inspiration; I would particularly like to thank Louise A., Arnau, Jo, Patricia, Alastair, Arianna, and Caro. Special thanks also go to Prof Sadie Creese, head of the Cybersecurity Analytics Research Group, for providing the opportunity to work under Prof Michael Goldsmith's supervision in her research group. Many thanks also go to the CDT program administrators, Mrs Janet Sadler, Mrs Maureen York, and Mr David Hobbs, as well as the CDT's director, Prof Andrew Martin, who have tirelessly worked to support me whenever I needed some help.

A DPhil cannot be written without the support of family and friends. I would like to thank my parents Zuzana and Michael, my sister Bernadette, and my larger family, for putting up with me even on grumpy days when it seemed my research was going backwards instead of forwards.

Equally, my friends have offered distraction and a positive environment. I would like to express particular thanks to Oleh Stupak, Pascal Schmalz, Arian Uruqi, Basil Oberli, Marko Mayr, Bernd Sturdza, Carlo Basbasi, Alex Heuzeroth, Lorella Kessler, Fabian Soltermann, Flurin Caviezel, Patrick Wyler, Fabian Schmidlin, Nikolas Blumenthal, Pablo Conca, Frithjof, Hoppe, Alexander Heuzeroth, Oliver Meyer, Lionel Tinner, Nicolò Gaggero, Michael Delahunt, and 357.

Finally, I would like to thank my good friends in the Czech Republic: Vojtěch Vasko and his wife Eliška, Jiří Bauer and Anna Štěpánová, Kristina Koščíková and Martin, Anna Marie Hradecká, Jarmila Grimmová, Blé, and Dig. Whenever I visited, regardless of how short the notice was, they

were always most welcoming and greatly efficient in helping me to relax, detach from work, and gain strength for any chapters that lay ahead of me.

Abstract

This thesis examines the impact of the cyberrevolution on the concept of neutrality. It understands neutrality as a political idea applied to a country's foreign policy, which is based on the definition in international law but has also been formed by historic precedents and international norms. Due to the lack of completeness of neutrality-related literature, a significant contribution of this thesis is the formulation of a taxonomy and basic principles of conventional neutrality theory before it pursues an exploration of how cyberspace affects state neutrality.

A central argument for conventional state neutrality formulated in this thesis is that state neutrality contributes to both the international stability of the global community and the national security of the implementing country. The research indicates that this argument is plausible for conventional neutrality theory as well as when considering the influence of cyberspace. The thesis contributes a comprehensive discussion of permanent and relative neutrality, including definitions of neutrality terms and a neutrality taxonomy, which is a significant research contribution for the understanding of neutrality—it may serve for the public and political discussions of neutrality, and as a framework for understanding decisions made by the government in a continuous tradition. Maybe even the government and the public administration can draw from the result of this thesis and use its findings in order to better explain various aspects of neutrality to the broader public and the international community.

With respect to cyberspace, neutrality is found to serve as a de-escalative element, which counteracts the escalative intuition of Buchanan's *cybersecurity dilemma*. This finding results from a case study covering the *RUAG Hack* in 2016, a cyberattack on a governmentally-owned defence contractor in Switzerland. Findings include the identification of indirect attribution and tactics for deterrence by means of publishing detailed technical reports without direct attribution by a neutral country's government. The

publication of a factual technical report by a neutral government significantly increases the potential cost for an attacker when deploying zero-days and also signals a significant cyberdefence capability to any future attackers, which may serve as a potential deterrent. Examples discussed in the thesis explain how “*legal signalling*”, a concept discovered and defined by this thesis, is an important de-escalative element that may contribute to a neutral’s trustworthiness and also as a deterrent.

This thesis also formulates the concept of *platform neutrality* applicable to globally operating social media companies. It illustrates that the concept of neutrality may well be applicable beyond states or international organisations, for example for non-state actors in a post-Westphalian system of global conflict and cooperation. The thesis puts these considerations into relation with the popular term of *network neutrality*.

The thesis is highly interdisciplinary: it is philosophically rooted in cybersecurity and computer science but applies social science methods: Several case studies, as well as a small number of semi-structured interviews provide further material for scrutinising and developing theory.

Statement of Originality

This thesis is written in accordance with the regulations for the degree of *Doctor of Philosophy*. The thesis has been composed by myself and has not been submitted in any previous application for any degree. The work presented in this thesis has been undertaken by myself, except where otherwise stated.

Parts of this thesis consist of work published at conferences or conducted as part of a *CDT Mini Project*. The former is the sole work of the author of this thesis; the respective research has been conducted while enrolled as a DPhil student at the University of Oxford and may, therefore, be considered to form part of the research conducted for this thesis. The latter is the output of a project conducted during the integrated “CDT year”⁴ of the doctoral programme in cybersecurity at the Department of Computer Science of the University of Oxford—it may equally be considered to form part of the overall research conducted in the process of obtaining the degree of *Doctor of Philosophy*.

Where work has been previously published or where it was conducted as part of a mini project, this is stated in the respective parts of this thesis. All work published at conferences is also included in Appendices A, B, C, and D.

⁴The term “CDT” refers to the *Centre for Doctoral Training in Cybersecurity* at the University of Oxford.

Contents

1	Introduction	1
1.1	Motivation for Writing this Thesis	2
1.2	Disciplines and Interdisciplinarity	5
1.2.1	The Discipline of Computer Science	5
1.2.2	Disciplinary Scope of this Thesis	7
1.3	The Term “Neutrality” and Switzerland	8
1.3.1	A Very Short Primer of State Neutrality	9
1.4	Research Questions	13
1.4.1	What is Neutrality?	13
1.4.2	What is Cyberspace?	16
1.4.3	Neutrality and Cyberspace	18
1.4.4	Research Questions and Conjectures	19
1.5	Thesis Methodology and Sources	22
1.5.1	Overview of Methods	23
1.5.2	Conjectures and Lemmas	24
1.5.3	Instrumental and Formal Definitions	25
1.5.4	Case Studies	25
1.5.5	Sources for Case Studies and Referncing	27
1.5.6	Interviews	29
1.5.7	The Word “Cyber”	31
1.6	Thesis Outline	31
1.7	Published Work	33
2	Cyberspace, Neutrality, and Global Politics	35
2.1	Switzerland and Neutrality	36
2.1.1	Swiss Politics	37
2.1.2	Swiss Neutrality, as seen by the Swiss Government	40
2.1.3	Neutrality Literature	42

2.2	International Relations Studies Concepts	45
2.2.1	International Relations Terms and Concepts	46
2.2.2	Cyberspace-related Concepts and Considerations	48
2.3	A Computer Science Perspective on Cyberspace	53
2.3.1	The Computer and Data	54
2.3.2	The Internet	55
2.3.3	Technological Considerations on Operations in Cyberspace . .	58
3	Neutrality as Defined in International Law	62
3.1	The Hague Conventions of 1907	63
3.1.1	General Obligations of a Neutral Party	63
3.1.2	Provision and Transition of Goods	64
3.1.3	Articles Referring to Communication Infrastructure	64
3.1.4	Rights of Neutral Parties	66
3.1.5	What is Not Covered in International Law	67
3.1.6	Application of Neutrality Law to Cyberspace	67
3.1.7	Conclusions for Cyberspace	70
3.2	The Tallinn Manuals	71
3.2.1	General Remarks on the Tallinn Manuals	72
3.2.2	Some General Terms	74
3.2.3	Rules Concerning Neutrality	75
3.2.4	Discussion and Conclusions on the Tallinn Manual	83
3.3	Further Work Discussing International Law	86
3.3.1	Publications preceding the Tallinn Manual	87
3.3.2	Monograph by Alexander Spring	90
3.3.3	Further Publications released after the Tallinn Manual	92
3.3.4	Key Findings on Further Legal Work	95
3.4	Conclusions for the Legal Perspective	96
4	Conventional State Neutrality: History and Theory	98
4.1	A Historical Case Study on Modern Neutrality	101
4.1.1	Historic Overview of Events	102
4.1.2	Manfred Hettling: Eine kleine Geschichte der Schweiz	110
4.1.3	Alois Riklin: Funktionen der schweizerischen Neutralität	114
4.1.4	Georg Kreis: Die Schweizer Neutralität	118
4.2	Active Neutrality and Recent Developments	120
4.2.1	The Emergence of a New Approach to Neutrality	125

4.2.2	Active Neutrality as Approved Foreign Policy Principle	128
4.2.3	Neutrality's Compatibility with a Seat in the Security Council	131
4.2.4	Reflections in the Media after Calmy-Rey's Resignation	136
4.2.5	Active Neutrality Following the Annexation of Crimea in 2014	138
4.2.6	Neutrality Following the Russian War in Ukraine in 2022 . . .	140
4.2.7	Main Case Study Themes and Conclusions	148
4.3	Neutrality History: Main Themes and Conclusions	153
4.4	Conventional State Neutrality Theory	156
4.4.1	A Taxonomy: Neutrality Definitions	156
4.4.2	Extended Taxonomy: Further Neutrality Lemmas	162
4.4.3	Intermediary Conclusions for State Neutrality	167
5	State Neutrality in Cyberspace	170
5.1	Theoretical Implications for Neutrality and Cyberspace	171
5.1.1	International Law Implications and Challenges	171
5.1.2	Permanent Neutrality Implications	176
5.1.3	Juxtaposition with Interviews	178
5.2	Examples of Activities related to Cyberspace	183
5.2.1	Attacks on the Red Cross in 2022	184
5.2.2	Engagements for International Norms	185
5.2.3	Example of " <i>Legal Signalling</i> "	187
5.3	The Case of the <i>RUAG Hack</i>	190
5.3.1	Findings of the RUAG APT Report	194
5.3.2	Public Disclosure of the RUAG Hack	197
5.3.3	Immediate Publication of Further Details in the News	199
5.3.4	Government and Parliament Press Release	202
5.3.5	Further public discussion of the case in May 2016	205
5.3.6	Media Coverage Following the Release of the RUAG APT Report	209
5.3.7	Later Publications	210
5.3.8	Analysis and Discussion of the Case	212
5.4	Conclusions for State Neutrality in Cyberspace	216
6	Neutrality as a Concept Beyond States	219
6.1	A Note on <i>Economic</i> Neutrality	220
6.2	Motivation for Platform Neutrality	221
6.3	Examples of Social Media Developments in 2020	222
6.3.1	Misinformation during the Coronavirus Pandemic	223

6.3.2	Reactions to the <i>Black Lives Matter</i> Movement	224
6.3.3	The US Presidential Campaign in 2020	225
6.3.4	Suggestion of Mitigation Mechanisms	226
6.4	Definition of Platform Neutrality	229
6.5	Discussion on Governance	232
6.6	Conclusions on Platform Neutrality	233
7	Conclusions and Future Work	235
7.1	Conclusions	236
7.2	Future Work	238
A	Published Paper: <i>On Neutrality and Cyber Defence</i>	240
B	Published Paper: <i>Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries</i>	249
C	Published Paper: <i>Platform Neutrality</i>	259
D	Published Paper: <i>Platform Neutrality and the Global Balance of Powers</i>	269
E	Interview Forms and Ethics	277
E.1	Interview Structure for State Neutrality	277
E.2	Interview Structure for Platform and State Neutrality	279
F	Interviews Conducted	281
F.1	Interview 1	281
F.2	Interview 2	282
F.3	Interview 3	284
F.4	Interview 4	286
F.5	Interview 5	288
F.6	Interview 6	290
F.7	Interview 7	290
F.8	Interview 8	292
	Bibliography	294

List of Figures

1.1	A visualisation of the research questions, conjectures, and arguments of this thesis.	14
1.2	Overview of the methodology for this thesis.	23
2.1	Illustrations of the conceptual components of a computer, derived from illustrations in Tanenbaum’s <i>Modern Operating Systems</i> (2014) [1], page 2 and page 5.	54
2.2	An illustration of the ISO layer model for networks, derived from an illustration in Tanenbaum’s <i>Computer Networks</i> (2011) [2], page 46. .	56
2.3	An illustration of the TCP/IP layers and common protocols used for Internet communication, derived from an illustration in Tanenbaum’s <i>Computer Networks</i> (2011) [2], page 48.	56
2.4	An illustration of interconnected networks, e.g., the Internet, including the aspect of routing. The graphic is derived from an illustration in Tanenbaum’s <i>Computer Networks</i> (2011) [2], page 62.	57
2.5	The different types of CNO: CND is defined as non-intrusive. CNE and CNA are intrusive and overlap. The graphic is taken from a paper by Stolz (2021) [3].	58
2.6	Illustration of intrusive operations in cyberspace, as published by Stolz in 2021 [3].	59
3.1	Implications of neutrality law for cyberspace.	68
3.2	Illustration of Neuman’s [4] WAF scenario.	94
4.1	A visualised summary of the findings on state neutrality and its taxonomy, as discussed in Section 4.4.	100
4.2	The functions of permanent neutrality, as defined by Riklin in 1991 [5].	115
4.3	The dimensions for permanent neutrality, as defined by Riklin in 1991 [5].	115
4.4	The functions of and dimensions for permanent neutrality, as presented in Subsection 4.1.3.	153

4.5	A visualised summary of the findings on state neutrality and its tax- onomy.	166
6.1	The functions of permanent neutrality, as defined by Riklin in 1991 [5] and presented in Chapter 4.	230
6.2	Platform neutrality functions, adapted from Stolz' definition in 2021 [3].	230

List of Tables

1.1	Summary of neutrality definitions, as defined in Chapter 4.	10
1.2	Interviews conducted as part of this thesis (anonymised).	30
4.1	Summary of neutrality definitions, as defined in Section 4.4.	99
4.2	Significant dates for the history of state neutrality in Switzerland. . .	103
4.3	Listing of articles of the active neutrality debate.	121
4.4	Listing of articles concerning Swiss neutrality following the Ukraine conflict.	122
4.5	Significant dates for the active neutrality debate.	124
5.1	Interviews conducted as part of this thesis (anonymised). The inter- view numbers with relevant content for this thesis are marked green. .	178
5.2	Timeline of the <i>RUAG Hack</i> case. Any events preceding the public disclosure of the case (3 rd May 2016) are extracted from the RUAG report [6] (see Subsection 5.3.1) and the timeline therein on page 32. .	191
5.3	Chronological listing (release date) of articles and publications from 2016 discussed in the RUAG Hack case study.	192
5.4	Chronological listing (release date) of articles and publications from 2018 to 2019 discussed in the RUAG Hack case study.	194

Chapter 1

Introduction

—“*Cyberspace does not lie within your borders.*”—

The above excerpt from John Perry Barlow’s *A Declaration of the Independence of Cyberspace*¹ exemplifies the fundamental change cyberspace has brought to security thinking: it is inherently revolutionary in nature since it virtually overcomes geographical boundaries and national borders seamlessly and instantly. Conventional dimensions of (kinetic) security are always determined by a spatial (or: *geographic*) component: land, air, sea, and even electromagnetism are limited by the geographical context in their effect and impact. Cyberspace, however, cannot be controlled by means of controlling a certain geographic space (or if so, then only in a limited sense).²

¹John Perry Barlow wrote down his *Declaration of Independence* while attending the World Economic Forum (WEF) 1996 in Davos (Switzerland) [7]. As evident from its content, it was written in response to the US Telecommunications Act of 1996, an early approach to governing the Internet and its use. It is an interesting and early example of the tension between a state and cyberspace *per se*, or more specifically, a struggle for power and control in this novel space. In this case, the struggle was between a freedom-oriented community of pioneers and a government. This example demonstrates parallels to the tensions between governments and large technology companies, in particular social media companies, which are covered later in this thesis.

²An elfish reader might argue that cyberspace is very well limited by geographic components. This is true as long as the installation of hardware is concerned but in terms of managing data—and the transmission thereof—this is virtually impossible unless basic principles of the core idea of common Internet technologies are broken or overruled. However, as is later discussed in Chapter 2, breaking these core components would yield the revolutionary character of the Internet—and, therefore, cyberspace—dysfunctional. It would stop the Internet and cyberspace from being what it is. At the same time, even if a state attempts to enforce limitations on communication within a specific geographical area this is almost impossible to fully achieve. Individuals could make use of satellite communication infrastructure, for example, in order to circumvent limited connection infrastructure on the ground. Or, in the case of existing communication infrastructure albeit heavily controlled, the very nature of Internet technology enables users to find workarounds to “great firewalls” or other censorship mechanisms.

The imminent question is how the emergence of cyberspace alters, limits, or enhances conventional concepts of security thinking and whether these concepts need to be updated or new ones have to be developed. Authors and researchers have addressed this from a political and global perspective, as is discussed in Chapter 2.

A concept that has found less attention by scholars is that of *state* neutrality. The term has, however, been used in connection with the Internet and cyberspace, namely when discussing the concept of *network neutrality* (see Chapter 6). Nevertheless, neutrality is a concept traditionally applied to states—the fundamental entities of sovereignty and power in international relations (IR). Neutrality is known as a concept of non-alliance, independence, impartiality, and expression of non-participation in foreign wars and conflicts. It has a long-standing history in Switzerland, which forms the most prominent example of a neutral country.

The upcoming sections explain the motivation and formal framing for addressing the topic of neutrality on the background of cyberspace. The thesis is inherently interdisciplinary combining topics from computer science, social science, and political science / international relations. It combines research methods from multiple domains. The approach is outlined and some specifics of the research conducted, with respect to methods, are explained. Also the research questions and assumptions are outlined in this chapter, as are some general methodological remarks on sources used for case studies. Finally, an overview of the upcoming chapters and of work published as part of this thesis is provided.

1.1 Motivation for Writing this Thesis

It is the aim of this thesis to illuminate the meaning of neutrality for global security, international relations, and the power dynamics within and between states, on the background of the revolutionary character of cyberspace. The primary focus of this thesis lies on neutrality as a concept applied to states, and how this concept is impacted by the emergence of cyberspace. However, since some scholars have argued that the state is no longer the sole sovereign entity for international relations theory,³ it might also be useful to consider neutrality as a concept beyond states—as has to some extent already been done with the formulation of the idea of *network neutrality* by Tim Wu in 2003 [9]—which is also discussed in this thesis (see Chapter 6), although it should be noted that this is not its main focus.

³Most prominently this has been done by Lucas Kello in 2017 [8], as is later discussed in Chapter 2.

Before delving into the specifics of neutrality and the research questions, however, it is useful to understand the general motivation for writing this thesis. As documented later, neutrality is a central concept for Switzerland’s identity. While participating in the introductory year of the *Centre for Doctoral Training in Cybersecurity* at the University of Oxford, the author of this thesis participated in a course on international relations and cybersecurity. Neutrality did not seem to be a concept that was present both in conventional international relations theory and with respect to considerations of cyberspace. Indeed, as the research in this thesis shows, the concept of modern-day permanent neutrality, as implemented by Switzerland, is under-reported in conventional international relations literature and beyond; it is not surprising, therefore, that also a research gap with respect to considerations on neutrality with respect to the emergence of cyberspace—or as it is called in this thesis: the *cyberrevolution*⁴—exists.

At the same time, neutrality is a topic that is heatedly debated by politicians and society-at-large in Switzerland—also in 2022 and beyond. The heated format of the discussions is often not based on a systematic understanding of what conventional neutrality entails—also due to the lack of a comprehensive theoretical framework for neutrality. Government publications on neutrality are scarce and date back to the millennial years. Even terms concerning neutrality are used chaotically, as is indicated by a newspaper article from 2022 written by Jorio in NZZ [10]: What is active, integral, differential, or armed neutrality? How does neutrality evolve? Is neutrality purely defined by an international law definition—or is there a normatively developed implicit definition of something like permanent neutrality? Public debates on Swiss TV are led on neutrality, even in 2023, as documented by Caminada on SRF.ch [11], where politicians strongly disagree on how neutrality should be implemented without a foundation in a comprehensive theoretical framework on neutrality; also, people from outside Switzerland have difficulties understanding what neutrality is. Is Switzerland still neutral after it condemned Russia’s “special military operation”—or: invasion—in Ukraine in 2022 and when it participates in sanctions? The Swiss government has difficulties explaining to the populus how neutrality and the government’s implementation of foreign policy are in-line, as was also documented by the aforementioned TV debate.

When considering the question of neutrality as applied by states, an inherent challenge is to define the countries that are considered neutral. The neutrality debate

⁴This term is used based on Lucas Kello’s definition of the term in his 2017 book *The Virtual Weapon*.

is very prominent in Swiss politics. Other countries that have declared themselves to be neutral have meanwhile abandoned this approach. Both Sweden and Finland declared their will to join NATO in 2022, and Finland has already acceded to the military alliance while Sweden is expecting accession. Austria, a further example of a neutral country, is an EU member state; its example is less interesting since it mostly relies on the narrow international law definition of relative neutrality. Switzerland, as outlined by Alex Spring in his work from 2014 [12], is the most prominent example that not only follows relative neutrality law but has a long-standing uninterrupted foreign policy practice of permanent neutrality, which is defined normatively. The discussion in Switzerland is more contentious than with other countries due to its more puristic implementation of neutrality. Similar to Spring, this thesis considers Switzerland to be the example *par excellence* of a neutral country. Its role as a neutral country is studied, and a comprehensive framework for neutrality is derived from this case.

The aforementioned challenges with respect to neutrality become even more complex when considering the cyberrevolution: As Kello discussed in his work from 2017 [8], cyberspace has brought about a systems revolution with respect to how global cooperation and conflict between states work. In such a revolutionary environment, what is the role of a neutral country, and how does it respond to the constant state of *unpeace*⁵ in cyberspace? If conventional permanent neutrality has a stabilising influence on certain conflicts between third parties, can a neutral country have a similar role in cyberspace? How does a neutral country respond to activities that affect its infrastructure or central businesses / organisations, even if these activities evolve below the threshold of war? The RUAG Hack is a prominent case of such a situation encountered by the Swiss government and serves as a case study in Chapter 5.

Conventional neutrality as well as neutrality with respect to cyberspace require further research—this thesis contributes significantly to both. In order to understand neutrality on the background of the cyberrevolution, conventional approaches to neutrality need to be studied first. This thesis provides a comprehensive theoretical framework for conventional neutrality, including normatively defined *permanent* neutrality and the international law concept of neutrality, which this thesis refers to as *relative* neutrality. The aim is to provide a foundation for decisions made with respect to neutrality but also for understanding neutrality—for the Swiss population, as a

⁵See Kello’s work from 2017 [8]: The state of *unpeace* denotes the constant level of malevolent activities in cyberspace, which are below the threshold of war.

foundation for political debates and globally in order to understand Swiss neutrality practice.

1.2 Disciplines and Interdisciplinarity

As outlined, this thesis is concerned with the concept of neutrality and, more specifically, how it is affected by the cyberrevolution. While the specifics of cyberspace relate more to the domain of computer science, considerations on neutrality might rather be found in international relations, political science, the social sciences in general, or even the humanities when considering philosophical and legal⁶ aspects. It is, therefore, natural that the disciplinary scope of this thesis is less one-sided than is generally the case when working within the boundaries of one specific discipline. While this thesis is hosted in a *Department of Computer Science*, it addresses questions that might more commonly be addressed in a university department of politics, philosophy, or international relations; it is written in a *Centre for Doctoral Training in Cybersecurity* addressing cybersecurity, an inherently interdisciplinary subject area, which does not yet provide well-defined methodological or disciplinary boundaries. Rather, it is characterised by a broad fusion of topics and research disciplines that, in one way or another, address problems of cybersecurity.

The following subsections discuss the boundaries of computer science and the disciplinary approach of this thesis.

1.2.1 The Discipline of Computer Science

In order to provide a minimum specification as to how the conventional disciplinary boundaries of computer science are commonly defined, it is useful to consult considerations on the philosophy of computer science.

Unfortunately, the philosophy of computer science is not a particularly well-researched field; computer science has rather loosely defined disciplinary boundaries. In fact, computer science as an academic discipline may be characterised by a lack of consensus on its disciplinary boundaries, including a lack of consensus on any generally accepted methods. A textbook on *The Science of Computing* published by Tedre in 2014 [13] explains the difficulty and outlines what is commonly practised in departments that claim they do *computer science* as follows:

⁶Some readers might rightfully intervene that the study of law and jurisprudence may also be considered to be a separate disciplinary branch, or also be considered to be part of the social sciences, depending on which aspects of the law are being studied.

“[...]there is no consensus on what computing as a discipline is actually comprised of. Asking ten computing researchers what computing as a discipline is will yield ten different answers. [...]aside from some central concepts and innovations, there is considerable disagreement with many aspects of computing as a discipline: for instance, opinions diverge about proper methods, subjects of study, or proper curricula for computing fields. [...]Some argue that computing is primarily a technical field that aims at cost-efficient solutions, and others argue that the field’s important contributions are theoretical by nature. Yet another school of thought argues that computing is an empirical science [...]”

Presumably, it is not a bold statement to claim that a *de facto* (i.e., instrumental) definition of computer science would consider any content that is related to computing and computers as legitimate and would pose no particular limitations on methods applied. This is supported by an article written by Anguis in 2021 in the *Stanford Encyclopedia of Philosophy* [14]:

“Computer science can accordingly be understood as a scientific discipline, in that it makes use of both deductive and inductive probabilistic reasoning [...]The thesis that computer science is, from a methodological viewpoint, on a par with empirical sciences traces back to Newell, Perlis, and Simon’s 1967 letter to Science [...]Since Newell and Simon’s Turing award lecture, it has been clear that computer science can be understood as an empirical science but of a special sort [...] Indeed, much current debate on the epistemological status of computer science concerns the problem of defining what kind of science it is [...]”

Therefore, computer science offers some level of ambiguity on how the limitations of research topics and methods are defined. In that sense, this thesis can be considered a computer science thesis, even if it uses social science methods: Its content is focused on questions arising from computers, the Internet, and what is called cyberspace. More specifically, this thesis is concerned with what is broadly understood as cybersecurity; i.e., questions with respect to security that have emerged on the basis of the existence of cyberspace.⁷ However, there is a certain convergence of methods commonly applied in computer science: Scientific testing of engineering constructs, theoretical reasoning (i.e., formal logic and mathematical proofs), the analysis of algorithms, etc. This

⁷A discussion on what cyberspace is is led later in Chapter 2.

thesis uses methods from social science, which is not unseen in computer science (e.g., when considering aspects of user friendliness or usability) but is nevertheless unorthodox.

1.2.2 Disciplinary Scope of this Thesis

As explained in the previous subsection, this thesis may be considered to be within the boundaries of computer science, although in an unorthodox way: It is the openness of computer science as a discipline and with respect to its methods that allows for setting this thesis in computer science while applying methods common in social science. Hosting this thesis in a social science, politics, or legal setting would unnecessarily narrow the potential considerations that could be brought forward due to the limitations of these disciplines with respect to academic orthodoxy.

The thesis topic is in cybersecurity; this domain is commonly understood as an interdisciplinary research area. For example, the Oxford University Press *Journal of Cybersecurity* describes it as “*research in the inherently interdisciplinary cyber domain*” on its website (2023) [15]. Among others, the following academic disciplines are listed on the website of the journal:

- *computer science and security;*
- *legal aspects of information security;*
- *political and policy perspectives;*
- *strategy and international relations.*

In that sense, this thesis may be understood to be in the domain of cybersecurity, which spans multiple disciplines. In terms of its disciplinary home, the thesis is in computer science—which can be seen to include cybersecurity. Cybersecurity is concerned with security considerations on the basis of interconnected computer systems, which is in-line with the scope of computer science as an academic discipline discussed earlier. The openness of computer science to empirical methods provides for the application of methods from social sciences and also enables thorough analyses. On the other hand, the experimental side of computer science allows for the formulation and suggestion of concepts and frameworks more freely. Finally, the philosophical-theoretical nature of some aspects of computer science also justifies reasoning beyond the conventional boundaries of social science methods and allows the formulation of

straightforward formal statements and lemmas. The exact impact of these considerations is outlined later in the section on the methodology applied (Section 1.5).

In conclusion, this thesis, while set in a computer science environment, draws from multiple disciplines, in particular with respect to the application of case study methods and its consideration of concepts commonly discussed in other disciplines. It may be considered interdisciplinary in that sense: A conventional computer science perspective would fail to provide a comprehensive picture of neutrality and cyberspace, as would a conventional social science or international relations perspective; important aspects that only arise when considering both social science and technology would be missed. The interdisciplinary approach of this thesis, drawing from multiple disciplines, provides a more complete picture and yields findings that are more adequate since technology and social aspects are combined to form a suitable abstraction. This approach is a necessity given the complexity and diversity of the topic of this thesis.

1.3 The Term “Neutrality” and Switzerland

Neutrality is, first of all, a philosophical term, which is applied to states in political science and international relations. This thesis mainly approaches the term neutrality from the perspective of a country or state—however, the term is by no means monopolised by such an application. As the *Oxford English Dictionary* [16] outlines (2022), the term has come into the English language from Latin and French origin. While the French origin dates to the 14th century, the Latin origin seems to be slightly older and dates back to the 12th century. The original Latin meaning of the word is an “*intermediate state or condition*” [16]. However, the term appeared in the English language as a translation from Latin again in the 14th century again, this time with an emphasis on “*political neutrality*” [16]—very similar to the term’s translation from French in the same century, which denoted as much as “*the state of not being on any side*” [16] and, again in the 15th century from French, the term denoted more specifically “*the attitude of a political power which does not participate in hostilities between two other powers*” [16]. The term was once again imported from French in the late 18th century with a scientifically-chemical application, which is of less interest to us: “*the fact or state of being chemically neutral*” [16].

This etymological history underlines a tendency of applying the term with a political emphasis, i.e., in the sense of *political* neutrality. Therefore, it has mostly been applied to the fundamental entities of modern international relations, namely states or countries. However, the etymological history also shows how the term may be used

more broadly, in the sense of an *intermediate state or condition* and *the state of not being on any side*. As explained later in Chapter 6, the term *network neutrality* does not focus on the political concept of neutrality that the term is most broadly used for. Rather, it denotes a type of *economic* neutrality. The focus of this thesis lies on the political idea of neutrality. Since the most common application of *political* neutrality is with respect to states, the main focus of this thesis lies on political neutrality as applied to states. However, there will also be a reflection on how the considerations on political neutrality could be applied to entities beyond states in Chapter 6.

In order to provide the reader with an understanding of some challenges political neutrality may face when applied to states and in order to explain the term neutrality, when applied to states, to the reader who may have limited knowledge of the term, the following subsection provides a very short overview of state neutrality.

1.3.1 A Very Short Primer of State Neutrality

As stated earlier, neutrality is a term that may be widely used but usually is applied in the sense of political neutrality. Most prominently, it refers to the political neutrality of states, which this thesis refers to as *state neutrality*. In this sense, neutrality is a concept of foreign policy. As outlined later on, it has been codified to some extent in international law and also provides for interesting discussions and analyses with respect to international relations—however, international relations often disregards the consideration of state neutrality as a factor in its major disciplinary theories (see Chapter 2).

State neutrality has most prominently been applied by Switzerland. This could be understood as “commonplace” knowledge about neutrality—it is presumably undisputed that Switzerland is the most prominent and long-lasting example of state neutrality—nevertheless, this statement is also backed numerous in the literature. For example, Alex Spring states in a monograph on neutrality in the 21st century:

“Switzerland is the classical example of a permanently neutral state. It is the only state that was already, in the 19th century, permanently neutral (with international acceptance) and has remained neutral up to the present time[...] Switzerland provided a fundus of state practices that shaped the understanding of permanent neutrality in international law[...]for a permanently neutral state, there is no doubt that Switzerland is still today the prototype of such a state”

Term	Definition summary
Neutrality	Philosophical / etymological term denoting impartiality, not restricted to a political / legal meaning.
State Neutrality	Neutrality in the sense of impartiality, when applied as a concept for states in the international “arena”.
Military Non-alliance	Independence of a state from an alliance system—not necessarily subject to not being on any side or restricted by any neutrality restrictions.
Relative Neutrality	State neutrality as defined in international law; strictly speaking in international law neutrality is always relative to a specific conflict.
Permanent Neutrality	Commitment of a state to remain neutral even before a conflict arises; norms-based.
Geostrategic Neutrality	Declaration of a territory / state as neutral based on its geostrategic relevance (such as for Switzerland in 1815).
Armed Neutrality	Not a type of neutrality. Denotes the necessity of a neutral possessing an effective defence capability, in order to credibly be able to uphold its neutral status.
Differential Neutrality	Permanent neutrality under the aspect of the state integrating itself into established international structures, such as the UN. Often refers to Swiss neutrality during its membership in the League of Nations (between the World Wars).
Active Neutrality	Similar to differential neutrality. Swiss neutrality as implemented since the early 21 st century. Term coined by Federal Councillor Micheline Calmy-Rey.
Integral Neutrality	Form of permanent neutrality which refrains from an integration into international structures due to their irrelevance and evolving international tensions. May be described as an isolationist approach in times of international instability.
Cooperative Neutrality	Term coined by federal Councillor Ignazio Cassis in 2022 and rejected by the Federal Council; it denotes a stronger formalisation of collaboration with western countries and alliance systems. Austria’s neutrality may be considered to be cooperative.

Table 1.1: Summary of neutrality definitions, as defined in Chapter 4.

Therefore, this thesis focuses mainly on Switzerland. The following paragraph provides a very brief overview of how Swiss neutrality came to be and how it was and is significant for Switzerland and the international community.⁸ An overview of neutrality definitions, as categorised by the case study in Chapter 4 is shown in Table 1.1, such that the reader can familiarise themselves with some of the terms used in this thesis. The definition of comprehensive elaboration of and discussion on these terms, based on a case study of neutrality practice, is a fundamental contribution of this thesis.

Swiss neutrality developed from a foreign policy principle of non-alliance, which has been applied by the Swiss *Old Confederacy* (pre-1848 Switzerland) since the *Marignano Defeat* in 1515. The Marignano Defeat marked the end of Swiss “great power politics” and subsequently spared the Old Confederacy from any major involvements in the Thirty Years’ War. The Westphalian System of sovereign states has since emerged as the system for international politics, as is documented in mainstream international relations textbooks⁹.

Modern-day Swiss neutrality emerged from the Vienna Congress in 1815, which reorganised European politics following the Napoleonic wars. The Vienna Congress declared that Switzerland should remain neutral due to its geostrategic significance, as a country located in the Alps and, therefore, controlling territory relevant to trade routes connecting northern Europe with the Mediterranean area. If this area would be controlled by or part of the influence sphere of a major European power, it would disturb the “*Balance of Power*”—and, thus, the stability of peace—between the five major European powers of the time: Austria, Britain, France, Prussia, and Russia.

State neutrality had not been specified in its meaning by the Vienna Congress. Rather, it was an abstract concept, combining ideas of independence, non-alliance, full sovereignty, a common interest by the major powers of that time (in the sense of a Balance of Power for international stability and peace), but also a requirement for an internal balance by non-alliance of a country with multiple linguistic and confessional groups, and a commitment to not use military means as an instrument of foreign policy. Furthermore, over time this included a commitment to a credible ability of self-defence (“*armed neutrality*”) and also impartiality with respect to international matters, as a consequence of Switzerland’s non-alliance.

⁸The historical dates and events may be found in major textbooks on Swiss history, such as by Kreis (2014) [17], and are further elaborated on in Chapter 4.

⁹For example, by Nye (2017) [18] or Heywood (2014) [19], see Chapter 2 for more details.

The Vienna Congress was not the first instance of the use of neutrality as a term with respect to the status of a country in relation to potential conflicts. While Swiss politicians tend to perceive Switzerland’s neutral status as something positive, ancient examples from Theucydides’ *History of the Peloponnesian War* [20] portray neutrality as something negative:¹⁰

The island state of Melos is said to have chosen to remain neutral during the Peloponnesian War—i.e., it did not want to partake in the hostilities and wanted to remain independent from either side of the hostilities; it refused to pay tributes to Athens even when threatened with a siege and an invasion. Athens did not want to accept Melos’ neutrality, since it anticipated that if it would not conquer Melos, Athens would be perceived as weak and other island states of the Delian League (led by Athens) might be tempted to rebel against the league’s hegemon. Melos was eventually conquered by Athens, all men were slain and the women and children enslaved. The Melian Dialogue provides an interesting case with respect to neutrality, which is very different to that known to be implemented by Switzerland: Melian neutrality is unsuccessful, Melos is conquered and the Athenians claim, “*the strong do what they can and the weak suffer what they must*”—or, in other words, “*might makes right*”¹¹.

In international relations, such a statement would usually be aligned with the realist school of thought, and there are many examples—most recently that of Ukraine—where such statements explain events in relation to international conflicts. How is it, though, that Switzerland has managed to implement its neutrality successfully since 1815 (and its military non-alliance since 1515) without suffering a similar fate? Are there factors that contribute to the successful implementation of neutrality? And how are these factors, and the implementation of permanent neutrality more generally, affected by the cyberrevolution? After all, cyberspace has been claimed to revolutionise

¹⁰The following examples of the fate of the island of Melos during the Peloponnesian War is commonly found in international relations textbooks, such as by Nye (2017) [18] and Heywood (2014) [19]. These were in fact where the author of this thesis received the pointers to the fate of Melos being an ancient example of neutrality (See Heywood (2014) [19] page 249 and Nye (2017) [18] page 26). Both textbooks, however, show that neutrality does not receive particular attention in major international relations theory and its related discussions and, if at all, the Melian example is taken as an indicator that neutrality is something that is very difficult to maintain and not a means in particular support of national security objectives of a state. The statements in the following, which go beyond the findings in the international relations textbooks already mentioned, refer to the fate of Melos and, in particular, the Melian Dialogue, as it is found in the original *History of the Peloponnesian War* [20] by Thucydides. Numerous translations are available, such as the one released as part of the *Oxford World’s Classics* series in 2021[21].

¹¹See Nye (2017) [18], page 26.

the “*Westphalian System*” of international relations that most conventional international relations are based upon.¹²

These questions are more clearly shaped into particular research questions in Section 1.4

1.4 Research Questions

As stated in the introductory paragraph of this chapter, the aim of this thesis is to understand how the concept of (state) neutrality is altered, limited, or enhanced by the emergence of cyberspace as a relevant security dimension. As the title of this thesis suggests, there are two fundamental terms that require clarification in order to address the core topic of this thesis: *neutrality* and *cyberspace*. In the following, Subsections 1.4.1 and 1.4.2 elaborate separately on the question of what these respective terms mean and what might be difficulties with respect to their definition and their understanding. Subsection 1.4.3 further elaborates on potential challenges when bringing these terms together.

Thereafter, Subsection 1.4.4 derives the respective research questions from the reflections in the previous subsections and formulates the specific questions and underlying conjectures, which drive the research of this thesis.¹³ An overview of research questions, conjectures, and arguments of this thesis is illustrated in Figure 1.1.

1.4.1 What is Neutrality?

As outlined, the inherent question when exploring the impact of the cyberrevolution on the concept of neutrality is: What is neutrality? Previously in this chapter, neutrality has been introduced as a term predominantly used in the sense of *political* neutrality (see Section 1.3). This thesis focuses on neutrality in that political sense. One exception is a short reflection in Chapter 6 on how political neutrality relates to network neutrality.

Apart from being a political concept, the imminent question for the understanding of neutrality is what the primary object of its application should be. As outlined in

¹²This claim has, among others, been made very prominently by Dr Lucas Kello in his book *The Virtual Weapon and International Order*, published in 2017 [8].

¹³The nature of the research question has been defined by means of consulting Lamont and Boduszynski’s publication on research methods in politics and international relations, published 2020 [22]. The chapters on research question formulation and research design have been particularly helpful for the adequate formulation of a research question. Furthermore, in a later stage, Yin’s book on case study research and its applications, published in 2018 [23], has been consulted for the purpose of reformulating the research questions.

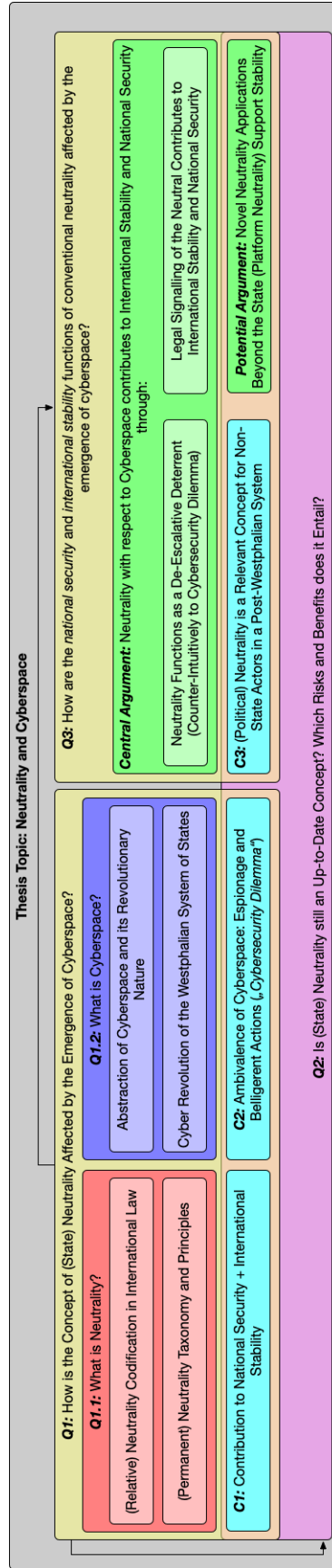


Figure 1.1: A visualisation of the research questions, conjectures, and arguments of this thesis.

Section 1.3, it is most commonly applied to political bodies. Of course, it may also be applied to entities, such as courts, mediators, or further parties. However, this thesis focuses on the impact the revolutionary character of cyberspace has on global politics and, therefore, the conventional focus of neutrality on its application as a concept for countries is a central interest with respect to the changes imposed to it by the emergence of cyberspace. This type of neutrality may be more accurately referred to as *state neutrality*.

As already explained in Section 1.3, the case example *par excellence* for state neutrality is Switzerland. As Spring [12] outlines in his monograph on neutrality law published in 2014¹⁴, there have been numerous examples of further modern-day neutral states. From the perspective of 2023, however, most former examples of neutral states no longer pursue neutrality or they have reduced their neutral status to concepts that are closer to military non-alliance than neutrality.

Hence, an inherent question when exploring the impact of the cyberrevolution on the concept of state neutrality has to be:

What is (state) neutrality, in particular with respect to the Swiss example of its implementation? What are its underlying principles?

A reflection on and analysis of how the emergence of cyberspace affects the concept of neutrality is only possible if an understanding is developed for *what* state neutrality is. In fact, a large part of this thesis is concerned with analysing and defining what state neutrality is (see Chapters 3 and 4).

The understanding of state neutrality is shaped by different disciplines. In particular, it is defined in international law but also by a state's policy decisions and depends on how a state understands its role as a neutral actor. Furthermore, neutrality cannot purely rely on the implementing state but is also shaped through norms that develop over time, which reciprocally shape the expectations of other states towards the neutral and are shaped by the expectations of other states. Spring states that the concept of neutrality "*gained its recognition through customary international law and is therefore, to a high degree, dependent on a constant practice of permanently neutral states*".¹⁵

Apart from the outlined different perspectives (international law, customary law, global politics) on state neutrality, neutrality may also be seen as taking different

¹⁴See page 105ff [12].

¹⁵See Spring (2014) [12], page 39.

forms. Spring (2014) [12] divides state neutrality into two main categories: *relative* and *permanent* neutrality. To some extent, these “types” of state neutrality influence one another and, to another extent, they also align to different perspectives on neutrality: Relative neutrality refers to the rules of neutrality codified in international law, while permanent neutrality is a more specific term for the form of neutrality, which is defined by norms, expectations, and customary international law. This thesis bases its arguments on the idea that permanent neutrality divides itself into further “types” of neutrality. A substantial contribution of this thesis is the specification of principles for these types of neutrality. Furthermore, it develops, through analytical derivation, formal definitions of neutrality “types” and, therefore, constructs a taxonomy of neutrality.

However, while this thesis may be able to provide an answer to a certain extent with respect to *what* state neutrality is, the answer will require further investigation, in order to elaborate on how neutrality is practised in—or affected by—cyberspace.

1.4.2 What is Cyberspace?

The previous subsection outlined the challenges connected with the definition of neutrality. This subsection provides some detail on the term cyberspace and its revolutionary character. First of all, a reflection on how cyberspace may be defined is provided. Chapter 2 is devoted to providing, among other things, a thorough discussion not only of what cyberspace is in terms of a definition but also provides an abstraction of how to think about cyberspace. However, it may quite safely be states that any definition of cyberspace must include the Internet or Internet technologies as a core component of cyberspace, and, depending on the specific definition of cyberspace used, includes devices, data, and software (potentially) connected or accessible. It is the Internet, which engenders the revolutionary character of cyberspace, since it allows access to information seemingly instantly and from any location in the world, as long as it has access to any other part of the Internet. It is exactly this characteristic of the Internet, which is at the core of the revolutionary nature, also with respect to many disciplines beyond computer science, such as law, politics, international relations, etc.:

Conventional thinking, e.g., the study of international relations, relies on a traditional understanding of information, time, and space: Before the emergence of cyberspace, information was usually tied to an object (e.g., a piece of paper). It relied on physically moving that information from one place to another—which included

a time component. Of course, the emergence of wired and wireless communication systems from the 19th century onward meant a significant change to this.¹⁶

Cyberspace in a broader sense would probably need to include “classical” telecommunication systems, including wired and wireless information transmission.

However, cyberspace in a narrower sense specifically relates to the Internet, the World Wide Web and its more dynamic approach to information exchange: Additionally to global communication, the Internet further brought about the revolution of dynamic information provision: Before the Internet, data needed to be requested and then sent. While this principle remains even on the Internet, it is seemingly no longer necessary to request a piece of information—as long as it is already present on the Internet and—usually—access is granted. Therefore, information is required dynamically, as the user requires it. However, there is a second essential dynamic component to the Internet: that of automation and, inherently, software and applications: The Internet does not only allow sharing of information in a dynamic and ubiquitous way but also allows the ubiquitous handling of data. In addition to previous telecommunication systems, this enabled a significant shift of appliances that were previously part of the “real world” outside cyberspace to be moved into cyberspace. The change of the medium would bring about automation but also virtually instant access.

In terms of security, this means that the whole way of—conventional space-oriented—thinking was affected: Conventional security thinking is shaped by geographically-focused considerations. Traditional (kinetic) means of impact and power projection are usually limited by geographical factors. This applies most prominently to land, air, and sea: factors such as the velocity of means (weapons, vehicles, forces), the geographical reach of weapon systems, etc. are decisive for impact generation and power projection. As already outlined, this reliance on moving through geographical—or conventional—space introduces a time component: relocating or deploying assets and forces takes time.

For the purpose of this thesis, a major revolutionary characteristic of cyberspace is seen in that it seemingly overcomes both space and time: information can be sent to any location with an Internet connection instantly and from any other place with an Internet connection. A vast amount of data is instantly accessible; many systems are directly or indirectly connected to the Internet. The emergence of cyberspace has revolutionised the mostly kinetically-focused thinking about security.¹⁷

¹⁶A thorough documentation and analyses of the changes imposed by international telephony and telegraph systems, which confirms these commonplace statements, may, for example, be found in two monographs published in 2002 [24] and 2007 [25], respectively, by Jill Hills

¹⁷The revolutionary character of cyberspace has been stated most prominently by Kello in 2017 [8].

On this basis, Lucas Kello declares cyberspace as revolutionary for international relations theory and its conventionally sole focus on the state as an entity of interest for international (in)stability: Kello suggests the introduction of non-state actors, such as large technology companies, as relevant global actors in the international arena¹⁸. This thesis largely relies on Kello’s considerations with regard to cyberspace, its revolutionary character, and its impact on international relations theory (see Chapter 2). Most notably, Kello’s findings show that the state—a (traditionally, since Westphalia) fundamentally geographically-oriented concept of power—might be affected by the cyberrevolution. However, in the previous section, neutrality was described as a concept most commonly applied to states—hence the question arises whether cyberspace fundamentally affects state neutrality.

1.4.3 Neutrality and Cyberspace

Neutrality has been introduced as a concept mainly applicable to states, stretching over several academic disciplines; cyberspace evolves around the Internet and automated dynamic information processing (i.e., programmable computing). Furthermore, the revolutionary character of cyberspace has been identified, since it fundamentally challenges conventional thinking due to its seeming elimination of space and time limitations—any information is available instantly and everywhere. At the same time, the core of a conventional state is its sovereignty over a specific geographical territory. The state also is the fundamental entity for scholars of international relations, who refer to the international system made up exclusively of states as the *Westphalian System*.¹⁹

The outlined baseline of cyberspace and neutrality inherently creates a tension between the geographically-oriented concept of state neutrality and the revolutionary character of cyberspace: How might the concept of (state) neutrality be affected by the cyberrevolution? Is neutrality still an interesting concept for a state and for the international community? How might the risks and benefits of neutrality change on the background of cyberspace—both from the perspective of the international community and the specific neutral state? And, since cyberspace has brought scholars as far as claiming that the state is no longer the sole entity of sovereignty that needs to

¹⁸See Kello’s *The Virtual Weapon* [8]

¹⁹It is—broadly—defined by international relations scholars as a system with sovereign states, where states form the fundamental unit of consideration for the study of international politics. It stands at the core of basic theoretical abstractions of global conflict and cooperation for events since the *Peace of Westphalia* in 1648. It is commonly covered in international relations literature for example by Nye (2017) [18] in his chapter *From Westphalia to World War I*.

be studied for the understanding of international relations, could neutrality potentially also be applied to non-state entities that are deemed to be relevant actors in a post-Westphalian system of global conflict and cooperation?

A central research question of this thesis, therefore, should cover the concept of neutrality on the background of the cyberrevolution. As has been outlined, Switzerland is the most prominent and long-lasting example of (permanent) state neutrality and, therefore, it makes sense to give it particular attention when attempting to understand neutrality and the impacts of cyberspace. The upcoming subsection elaborates on the formulation of the core questions for this thesis.

1.4.4 Research Questions and Conjectures

The previous subsections outlined a fundamental tension between the concept of state neutrality, which is based on conventional geographically-oriented ideas of state and sovereignty, and the revolutionary character of cyberspace. From the discussion and the motivation in Section 1.1, the following central question for research arises:

Question 1 (Central Research Question). —*How is the concept of (state) neutrality affected by the emergence of cyberspace?*—

And an evident follow-up question to this central research question that comes to mind—in the sense of a critical “*so what?*” response to the relevance of neutrality—is the following secondary research question:

Question 2 (Secondary Research Question). —*Is (state) neutrality still an up-to-date concept—in particular on the background of the emergence of cyberspace? What risks and benefits does it entail?*—

The questions above, in particular the central research question, function as the guiding element of research in this thesis, illuminating the path to a better understanding of the concept of neutrality on the background of the emergence of cyberspace. The central research question is exploratory²⁰ in nature; the secondary research question suggests a clear answer (in the sense of “*yes*” or “*no*” with respect to the question of relevance)—it is assumed that the answer is a “*yes*” and the more interesting aspect of *why* this is the case should be a deduction from outputs to the central research question—both questions are, therefore, overlapping. A clear priority

²⁰As explained by Lamont and Boduszynski in 2020 [22] in the respective chapter on research questions.

in this thesis is given to the central research question and the specific research question formulated further below. The secondary research question is formulated since results yielded by the work on the two previously mentioned questions (Question 1 and Question 3) may often provide interesting insights also with respect to Question 2. While it does not strictly adhere to conventional requirements for a research question in the sense of international relations or political science, it is nevertheless an important additional “*fil rouge*” for this thesis.

The questions stated above yield further questions as an immediate consequence: As explained in the previous subsections, gaining a thorough understanding of neutrality and cyberspace is an essential first step. Thereafter, more specific questions may become the focus of research, when exploring the impact of cyberspace on the concept of neutrality and its relevance. The following follow-up questions are stated as a direct consequence of Question 1:

Question 1.1 (Follow-up question on neutrality). — *What is (state) neutrality? How is it defined and what fundamental properties does it have?*—

Question 1.2 (Follow-up question on cyberspace). — *What is cyberspace? How may it be abstracted in terms of its revolutionary character, its functioning, and its impact on conventional (security) thinking?*—

Naturally, no final and absolute answer to any of the questions stated is possible; the aim is to establish a better understanding of how neutrality is affected by cyberspace, not to provide definitive answers.

Examining the topics raised by the questions above yields definitions and principles for state neutrality and its “subtypes”, such as relative neutrality and permanent neutrality. A core contribution of this thesis is the formulation of a taxonomy for neutrality, including definitions and “principles”, which are formulated under the term “*Lemmas*”. Furthermore, answering this questions requires formulating an abstraction of cyberspace and defining its revolutionary character.

The central conjecture for Question 1.1 is formulated as follows:

Conjecture 1. Conventional state neutrality contributes to international stability and to the national security of the neutral country.

This thesis, through its research on state neutrality, suggests that this is the case.

Furthermore, the examination of cyberspace, as outlined in Question 1.2, suggests the following conjecture:

Conjecture 2. Cyberspace yields an ambivalence with respect to the distinction between espionage and belligerent activities.

In order to elaborate on Conjecture 1, a large amount of research is required, which is provided in Chapters 3 and 4. Conjecture 2 is a more or less straightforward conclusion from third-party work, which is discussed in Chapter 2.

In order to examine the impact of cyberspace on the concept of (state) neutrality, the impact of cyberspace on state neutrality's national security function (for the neutral state) and the international stability function should be examined, as stated in Conjecture 1.

Furthermore, relying on Conjecture 2, particular attention should be given to the ambivalence between belligerent activities and espionage operations in cyberspace.

Therefore, the following more specific research question is selected:

Question 3 (Specific Research Question). —*How are the national security and international stability functions of conventional neutrality affected by the emergence of cyberspace?*—

The main argument of this thesis is that, on the background of Conjecture 2, state neutrality contributes to international stability and the national security of the neutral country. As explained later in this thesis, this seems counter-intuitive when considering the *cybersecurity dilemma* formulated by Buchanan in his 2017 book [26], as is discussed in detail in Chapter 2. However, the thorough analysis of cases in Chapter 5 illuminates how neutrality can break the escalation pattern formulated in the cybersecurity dilemma.

A last note with respect to the considerations of the previous subsections is required, when considering the secondary research question (Question 2): First of all, both Conjecture 1 and Conjecture 2 are also essential for answering Question 2. Also, so far, it has been assumed that state neutrality is affected by the emergence of cyberspace as a concept for states. However, due to the reflections introduced in Section 1.4.2 with respect to novel (non-state) actors being relevant in a post-Westphalian theoretical conception of global affairs, one could also consider, whether neutrality is a relevant political concept for non-state entities in a post-Westphalian system. While a full investigation into this topic would be beyond the scope of this thesis, the following conjecture is nevertheless assumed:

Conjecture 3 (Platform Neutrality). (Political) Neutrality is a concept that bears relevance in cyberspace with respect to non-state actors of a post-Westphalian system, in particular with respect to global social media companies.

This conjecture may also be considered an interesting statement with respect to illuminating matters raised by Question 3: This thesis suggests a potential argument to be made in favour of a concept called “platform neutrality”, which is introduced in Chapter 6, and applies the concept of political neutrality (in parts) to large social media companies in their role as non-state actors in a post-Westphalian system.

As stated previously, reasoning in favour of Conjecture 3 would deserve a thesis of its own. This thesis will nevertheless provide some indications as to why this conjecture could be assumed to hold. By doing so this thesis also provides a further indicator for the continued relevance of neutrality, also beyond Switzerland and conventional states.

Figure 1.1 illustrates the questions, conjectures, and arguments outlined and also shows their mutual relations: It shows an overlap of Question 2 with both Question 1 and Question 3. Moreover, Question 1 is the core of the thesis, Question 2 and Question 3 are deduced from it. In this sense, it also shows how all conjectures illuminate two questions each.

The main argument (and also the “potential argument” to be made for platform neutrality, which is indicated by this thesis) results from the investigation of the specific research question, Question 3. Question 1.1 and Question 1.2, finally, are not considered questions of their own but are inherent follow-up questions of the exploratory nature of Question 1. As discussed, they yield essential insights for the conjectures, the argument of this thesis, and the formulation of the other questions.

1.5 Thesis Methodology and Sources

The interdisciplinary nature of this thesis has been outlined in Section 1.2. After having introduced the research questions in Section 1.4, this section outlines what methods are applied in order to investigate the research questions.

This section first provides a general overview of the methods applied and how they fit into the greater (inter-)disciplinary and subject philosophical context relevant for this thesis. Furthermore, some reflections on the usage of terms, such as *conjecture*, *lemma*, or the tension between formal and instrumental definitions are brought forwards. Thereafter, an overview of the application of methods for empirical research applied in this thesis is provided: Subsection 1.5.4 explains this thesis’ approach towards case study research, Subsection 1.5.5 outlines some specifics with respect to sources used for case studies conducted in this thesis, and Subsection 1.5.6 explains

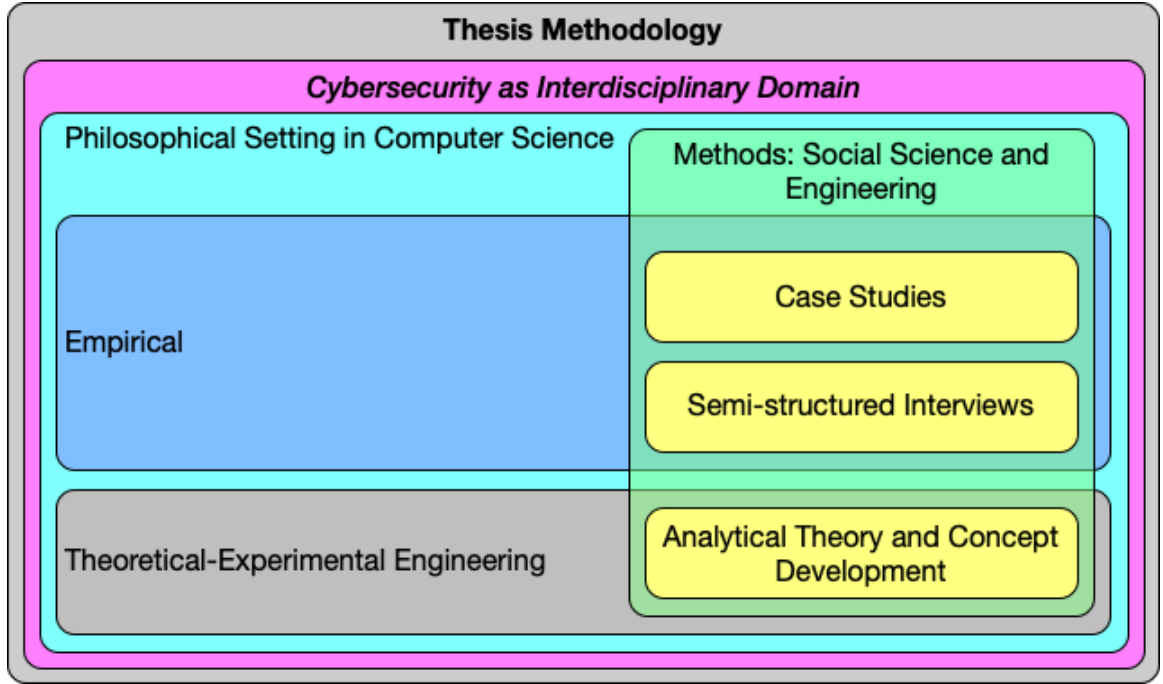


Figure 1.2: Overview of the methodology for this thesis.

how interviews were conducted in the context of this thesis. The section is closed by a discussion on the usage of the word “cyber”.

1.5.1 Overview of Methods

Having already introduced the (inter-)disciplinary context for the research conducted in this thesis, Figure 1.2 provides an illustration hereof and provides an overview of the methods applied:

As mentioned, this thesis is conducted in the interdisciplinary domain of cybersecurity and is philosophically “hosted” in computer science due to the background of the author and the methodological flexibility of such a setting. Section 1.2 briefly discussed the philosophical disciplinary understanding of computer science: It is understood as an empirical science, or as engineering, or as formalised experimentally driven research. In Figure 1.2 these approaches for computer science research are slightly adapted: While the empirical branch remains, the other two branches are combined into one: the engineering aspect is combined with the more formal side of computer science. It should be noted, however, that in this thesis there will not be any formal methods applied in the strict sense of computer science. Rather, this encompasses the formulation of theoretical definitions and lemmas, which have a certain formal character but are mainly used in order to form a theoretical understanding of

the world. Therefore, this “combined” branch in Figure 1.2 should be understood to be mainly situated in engineering science, with some components of a minimal formal methods character.

Within these branches of computer science research, the social science methods applied in this thesis are situated and integrated as follows: Both case studies and semi-structured interviews are *empirical* methods applied in this thesis and they are covered in detail in Subsections 1.5.4 and 1.5.6. The third method applied is that of a more theory-based analysis, including the advancement of theory or, as it is called in this thesis: *concept development*. On the one hand, this may include the analytical observation of existing theories, for example of the legal theory of (relative) neutrality. Furthermore, this method is applied, when constructing concepts of neutrality, which may be a result of findings generated by case studies or interview data, or even of reflections on analytical theory. This “generation of theory” is an active design and engineering of theoretical concepts, which the author of this thesis believes is methodologically best situated in the computer science branch of engineering.

1.5.2 Conjectures and Lemmas

When outlining the research questions in this chapter, the word “*conjecture*” was used to denote some assumptions made that are supported with the work made in this thesis. A common and related term often used in international relations theses is “*hypothesis*”. However, hypotheses consist of a set of variables that are then tested by means of historical case analyses. This thesis, however, aims at providing a better understanding of theoretical concepts and juxtaposes these concepts with their real-world applications. The use of hypotheses in this sense would not be appropriate for the research conducted.

A conjecture, in the context of this thesis, denotes a theoretical assumption or idea to explain what is seen in the real world. It does not necessarily include variables, since the work conducted in this thesis is of a more foundational character; work from this thesis might be used in later research to formulate hypotheses that can be tested. The main contribution of this thesis, however, is to advance understanding of neutrality and of the effect of the cyberrevolution on it.

A further term that is used later in Chapter 4 and Chapter 5 is “*lemma*”. This thesis aims at providing a formalised understanding of neutrality and as such states lemmas that explain tendencies of or relations between neutrality definitions, in order to provide a comprehensive taxonomy as a basis for neutrality theory. Lemmas are

formalisations of conclusions or findings in this thesis—they formally express what is expected and plausible on the background of the research conducted in this thesis.

1.5.3 Instrumental and Formal Definitions

A major contribution of this thesis to academia is formalising definitions of various terms in the neutrality discussion. When conducting case studies, a difficulty arises with respect to the analysis and deduction of definitions: Should the foundation be theoretical or practical / empirical? In the discussions of this thesis, the tension between formal (i.e., theoretical) and instrumental (i.e., based on pragmatic decisions) is a constant theme: Some definitions might provide a puristic, academic understanding—nevertheless, the text also discusses how they are implemented in practice. A common theme is that the implementation of neutrality might intuitively appear to include many contradictions with the formal definitions. An essential contribution of this thesis to the application of neutrality concepts in the real world is to understand how these applications make sense, also theoretically, although they may intuitively appear to be contradicting a formal definition made earlier. Furthermore, the formal definition of a term, concept, or lemma always evolves along the instrumental definition: Theory only has a value when it provides a valid abstraction of the real world. This thesis contributes to providing such a valid abstraction for neutrality and cyberspace.

1.5.4 Case Studies

As outlined, case studies are an important method applied in this thesis. They originate from the social sciences and this thesis mainly relies on the work of Robert K. Yin on case study research from 2018 [23]: Case studies do not provide an absolute truth but possible explanations that are scrutinised and reflected upon. Therefore, the language for case studies (and social science research in general) will be less absolute than is common in most Computer Science theses. According to Yin’s 2018 book [23], case studies *explain, describe, illuminate, enlighten, illustrate, etc.*

In the following, some main points of his work are summarised from his monograph from 2018 [23], in order to provide an understanding of the methodological foundations for the research conducted in this thesis.

Yin defines case studies in his 2018 work [23] as:

“empirical method that

- *investigates a contemporary phenomenon (the “case”) in depth and within its real-world context, especially when*
- *the boundaries between phenomenon and context may not be clearly evident.*

In other words, you would want to do a case study because you want to understand a real-world case and assume that such an understanding is likely to involve important contextual conditions pertinent to your case”.

This is exactly what this thesis attempts to do in terms of understanding neutrality and the impact cyberspace has on it as a concept. On the one hand, this thesis generates an understanding of what neutrality is. Furthermore, it uses case studies, in order to identify how this understanding of neutrality is altered by challenges posed by the emergence of cyberspace. In this sense, the historical analysis of the characteristics of neutrality in Chapter 4 as well as the review of legal definitions and work on neutrality in Chapter 3 may be considered case studies—although the latter also bears some characteristics of the mentioned analysis of theory and development of concepts.

Yin further says [23] that a

“case study

- *cope with the technically distinctive situation in which there will be many more variables of interest than data points, and as one result*
- *benefits from the prior development of theoretical lemmas to guide design, data collection, and analysis, and as another result*
- *relies on multiple sources of evidence, with data needing to converge in a triangulating fashion.”*

These lines form a good summary of the methodological approach taken in this thesis with respect to understanding neutrality and cyberspace: Experiments on neutrality are difficult to conduct; by thoroughly analysing a case only a convergence into a certain direction but not an *absolute* statement is possible. Hence, case studies are ideal for the type of research conducted in this thesis. In some sense, the whole thesis may be seen as a large case study on the impact of neutrality on cyberspace, comprising multiple nested case studies, as well as interviews and analyses of existing theories and concepts. In fact, Yin also formulates that this “nested” case study is a valid form of case study research.

Yin further explains elements necessary for case study research design [23]:

“

1. *A case study's questions;*
2. *Its propositions [or: conjectures], if any;*
3. *Its case(s);*
4. *The logic linking the data to the propositions; and*
5. *The criteria for interpreting the findings.*

”

This chapter has previously already addressed questions and propositions (or: conjectures); the cases are outlined later in this chapter (see Section 1.6); the “logic linking” happens throughout this thesis when matching patterns and finding explanations, as well as the criteria for interpreting—these shall mainly rely on identifying and addressing rival explanations.

1.5.5 Sources for Case Studies and Referncing

As Yin outlines in his 2018 book on case study research and practice [23], a case study may draw from various resources: Newspaper articles, statements made by individuals, or any other types of publications as long as they are critically reflected on their validity and usefulness and provide discussion insights on the topic illuminated by a case study.

This thesis often makes use of non-academic publications, since the amount of comprehensive academic publications in the field of neutrality theory is limited. Even where academic literature is consulted, it is sometimes used as an input for case study research: Chapter 3 reflects on relative neutrality as defined in international law. It draws from original texts of international law for a critical first reflection, but also discusses academic contributions to neutrality law with respect to cyberspace; it critically scrutinises the validity of these contributions in order to provide a comprehensive understanding of the implications for and challenges to neutrality law. The discussion in Chapter 3, in this sense, is a case study with legal texts and academic literature, as well as a formalised text book from an alliance (the Tallinn Manuals from 2013 [27] and 2017 [28]) as input.

Chapter 4 and Chapter 5 often make use of media articles published in newspapers or on-line, since they provide a valuable track record of the respective neutrality

debates and cybersecurity events; the articles also outline how neutrality is perceived and reflected upon in the political and societal discussion, providing important pointers as to how neutrality can be formalised, how it is understood in society or by thinkers, and what impact certain events or policy decisions had on it as a concept. Since the Swiss government is likely to be very careful about releasing any publications on neutrality due to the contentious debate and to avoid potentially self-imposed restrictions on foreign policy options, sources such as official government brochures or official statements on websites have to be included in the case studies: In absence of a comprehensive elaboration of the government on neutrality, these provide a small number of insights as to how neutrality is practiced and conceptualised by politicians in the government.

Finally, a note has to be made on how these various resources are referenced. Even in a single discipline, various styles for referencing exist, and the discussions on which is more useful are contentiously led. This thesis draws from multiple disciplines, which increases the scope of options when referencing. A simple solution is to rely on what is common in the host department of this thesis: computer science. Indeed, the referencing style applied for this thesis is that of the *Institute of Electrical and Electronics Engineers*²¹ (IEEE) which is commonly used in computer science departments around the world and for many impactful computer science publication formats.²² Since this thesis draws from multiple disciplines, however, it is also useful to consider the referencing styles in social sciences: For readers of social science literature, it is often useful to know the author and year of a piece of work, in order to judge its context. Hence, this thesis adopts a merged approach. On the one hand, the IEEE style for referencing is used; references are provided in the text by means of a number in square brackets (e.g.: [0]); the numbers are listed at the end of the document with the full reference details. Furthermore, the author and date of the work concerned are usually mentioned in close proximity to the square bracket reference in the main text of the thesis, in order to provide the reader with some context of a source.

²¹See <https://www.ieee.org/>.

²²For an overview of the referencing style guidelines, the reader is pointed to IEEE’s referencing style guide from 2018 [29]. Furthermore, a comprehensive overview is also provided on the website of Victoria University (Melbourne) as accessed in 2023 [30], see: <https://libraryguides.vu.edu.au/ieeereferencing>.

1.5.6 Interviews

A further important method used in this thesis is that of semi-structured interviews. While it is not used as a primary method for forwarding knowledge, due to the small number of interview participants that was gathered during the process of writing this thesis, the interviews are used to reflect on research findings in this thesis: Participants were specifically asked to state their views on neutrality in general, on state neutrality on the background of cyberspace, and sometimes also on the idea of platform neutrality.

The specific method used for conducting the interviews is that of semi-structured interviews, as outlined in Chapter 7 of *Research Methods in Politics and International Relations* by Lamont et al. (2020) [22]:

“In semi-structured interviews, you pose a set of open-ended questions, and depending on the response, you may diverge from your planned questions with more specific follow-up ones. Given the flexibility for the researcher to delve into greater depth on particular points raised in the interview, the semi-structured interview is the most common interview format used by researchers in PIR [politics and international relations]. Semi-structured interviews are particularly valuable because the phenomena that are of interest to scholars in PIR – political developments and events, the foreign policies of states, and the behaviour of international organizations, multinational corporations, and civil society organizations – often require us to gain deeper insight into complex social processes. Common interview subjects for semi-structured interviews are often important decision-makers and other experts”.

As stated by Yin [23] though, interviews are often subject to bias—nevertheless, they are a valid input for case studies. In this thesis, they are mainly used for reflections on the advancement of theories (i.e., to reflect on and scrutinise discovered convergences in case studies) and also to point towards additional points that may not have been revealed and discussed in the case studies.

Any interviews conducted as part of this thesis followed the University of Oxford’s CUREC (Central University Research Ethics Council) process.²³ Data related to the conducting of interviews and CUREC is listed in Appendix E.

²³See: <https://researchsupport.admin.ox.ac.uk/governance/ethics/committees/curec>

No.	Interview Date	Background Interviewee	Topic
1	2017/03/27	A Swiss Public Official	State Neutrality
2	2017/04/11	A Swiss Public Official	State Neutrality
3	2017/04/13	A Swiss Public Official	State Neutrality
4	2018/03/26	A Swiss Politician and IT Entrepreneur	State Neutrality
5	2021/12/09	A Swiss Retired Diplomat and NGO Affiliated	Platform Neutrality, State Neutrality
6	2021/12/19	A UK Cybersecurity Expert and NGO Affiliate	Platform Neutrality, State Neutrality
7	2021/12/23	A Swiss NGO Affiliate	Platform Neutrality, State Neutrality
8	2021/01/05	A German NGO and Think Tank Affiliate	Platform Neutrality, State Neutrality

Table 1.2: Interviews conducted as part of this thesis (anonymised).

Interviews were conducted as semi-structured interviews with experts from different backgrounds. A total of eight interviews were conducted. An overview is shown in Table 1.2. The interviews are anonymised and numbered according to the date when they were conducted. The table also shows a very rough description of the background of the interviewee: As evident, civil servants, employees of NGOs, researchers, entrepreneurs, diplomats and politicians were interviewed who were deemed to enrich the findings of this thesis with their expertise. The interview contents are provided in Appendix F, according to their number. The interviews were conducted either in person or online. Interviews 1–3 were conducted as part of a mini-project preceding the initiation of the research specific to this thesis but during the time, when the author was a student of the CDT in cybersecurity so the content may be used for this thesis too. Those interviews were recorded and transcribed—the relevant parts have been summarised and are available in the aforementioned appendix. All remaining interviews were conducted specifically for this thesis, and no recordings were made, although hand notes were taken, which are provided in the appendix. The notes are minimally redacted and not thoroughly discussed in this thesis. As outlined earlier, they are occasionally used, when reflecting on the relevance and usefulness of the results of case studies included in this thesis and are, in that case, specifically referred to. The interviews that were recorded by means of notes are provided in the appendix; the contents are partially in German or in English, depending on the language spoken by the interviewee.

1.5.7 The Word “Cyber”

This thesis follows the approach common in the cybersecurity analytics research group in the Department of Computer Science at the University of Oxford: “Cyber” is, generally, considered a word that can only be written concatenated with another word, e.g., cyberrevolution, cyberattack, cybersecurity, etc. The rationale behind this approach is that “cyber” per se does not denote anything; it usually references the meaning of cyberspace. Hence, providing it as a separate word in the text is useless: it only derives a full meaning when concatenated with a second word.

Yet, there might be exceptions in the text: When referencing terms used by other authors, the text occasionally uses “cyber” as a standalone word in order to provide consistency with the terms of another author discussed in the text.

1.6 Thesis Outline

This section aims to provide an overview of the content of this thesis and to outline, which questions are addressed in which chapters through which methods. The overall thesis may be understood as a “meta” case study in the sense of the Question 1. Its sub-parts are made up as follows:

As outlined in Section 1.4, the central research question has two direct follow-up questions, which are concerned with understanding neutrality and cyberspace. The first chapters target these follow-up questions: Chapter 2 might be considered similar to a “literature review” section of a social science thesis or a “related work” chapter in computer science. However, it is more than that: It first provides a short overview of some key concepts of neutrality and necessary knowledge about Switzerland concerning neutrality—this first part is indeed similar to a classical literature review. This very basic knowledge about Switzerland and neutrality (the knowledge rooted in research concerning the latter is very limited) sets the stage for choosing key concepts from international relations literature relevant to this thesis’ conceptualisation of cyberspace. This is done alongside a computer science-oriented selection of the key concepts that make up the Internet and what is intuitively understood under the term cyberspace. As such, Chapter 2 may be understood as addressing Question 1.2 (on cyberspace) using “analytical theory and concept development”.

Thereafter, Chapters 3 and 4 provide thorough case studies that address the understanding of neutrality, i.e., Question 1.1. As already briefly mentioned, state neutrality may be divided into *relative* and *permanent* neutrality. This division is more closely outlined in Chapter 2. The consequence of this division is that Chapter 3

is devoted to relative neutrality, while Chapter 4 explains the concept of permanent neutrality and some of its principles. Relative neutrality is mainly explored using an extended case study of international law, both concerning conventional territorial thinking and with respect to the implications of cyberspace. The considerations on relative neutrality and cyberspace consist of two case studies: One is our own understanding of the challenges posed by cyberspace, and another is a critical reflection (in the sense of a case study) of the implications of what is written in the Tallinn Manual—a guidebook for the application of international law in cyberspace—and further literature claiming to address (relative) neutrality with respect to cyberspace.

Chapter 4 then provides a thorough case study on the term of permanent neutrality: It relies on historical precedents and further sources, in order to deduce patterns of permanent neutrality principles that the reality of state neutrality presumably converges. Chapter 4 culminates by providing a taxonomy of neutrality terms and related lemmas, which this thesis understands to form *neutrality theory*—it is a key output of this thesis, albeit not concerned with the specific of cyberspace, and closes an important gap in the sense of a prerequisite for reflections on how this theory of neutrality is affected by cyberspace.

Chapter 5 forms the core of this thesis: It synthesises the outputs of the previous chapters by providing:

1. A critical reflection on the findings of the previous two chapters with respect to the understanding of cyberspace gained in Chapter 2 as well as on the background of the case studies and analyses of neutrality from Chapters 3 and 4, as well as reflecting the findings with the interviews conducted. This may be understood as analytical theory and concept development;
2. in combination with the previous point an advancement of the understanding of what neutrality could mean with respect to cyberspace through the consultation of different examples of neutrality practice in the cyber era;
3. in combination with the first point and in the sense of analytical theory and concept development, an enhancement of how “legal signalling” is an example of de-escalating legislation employed by Switzerland as a neutral country;
4. a case study on the *RUAG Hack*, which occurred in 2016, in order to gain an understanding of how a neutral country responds to critical cybersecurity incidents with state actors;

5. concept development through all of the previous points with respect to the central research question and a reflection of the theoretical findings and case studies with respect to statements from interview participants.

As already outlined, this thesis also wishes to provide a suggestion on the potential of the future development of the term neutrality. With respect to Question 2 and the potential argument (see Figure 1.1) and on the background of recent developments with respect to social media platforms and their regulation, the concept of *platform neutrality* is briefly introduced. As already outlined, providing a thorough study with respect to the validity and potential of this concept is definitely beyond the scope of this thesis and would presumably deserve a thesis of its own. Chapter 6 also provides a very brief discussion of and differentiation from the term *network neutrality*, in order to explain how its conception of neutrality is fundamentally different from the *political* understanding of the term in this thesis.

Chapter 7, finally, concludes the thesis by providing major findings, also and particularly of the aforementioned *meta*-case study. It also provides suggestions for future work, for example with respect to platform neutrality.

1.7 Published Work

Over the evolution of this thesis, the author published the following papers at double-blind peer-reviewed conferences. This forms the standard method of research output and advancement in the domain of computer science—paper acceptance is an indicator of the quality of the work and the interest of the community in the topics researched.

1. 2019: *On Neutrality and Cyber Defence*; European Conference on Cyber Warfare and Security (ECCWS), see Appendix A;
2. 2021: *Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries*; International Conference on Cyber Warfare and Security (ICCWS), see Appendix B;
3. 2021: *Platform Neutrality—A Solution for the Social Media War?*; International Conference on Cyber Warfare and Security (ICCWS), see Appendix C;
4. 2021: *Platform Neutrality and the Global Balance of Powers*; International Conference on Computational Science and Computational Intelligence (CSCI), see Appendix D.

The first paper also provides content relevant to Chapters 3, 4, and 5. The second paper particularly influenced some of the contents of Chapter 5, while the last two papers are important indicators for the potential future further evolution of the term of neutrality, as is discussed in Chapter C.

Chapter 2

Cyberspace, Neutrality, and Global Politics

As outlined in Section 1.6, the aim of the current chapter is, on the one hand, to provide a short overview of Switzerland and Neutrality, similar to a literature review. This is done in Section 2.1. This is necessary since several case studies contained in this thesis are conducted on topics connected with Switzerland—as the most prominent and long-lasting example of a permanently neutral country—and, therefore, knowledge about Switzerland provides case study context.

The more interesting and complex part of the chapter follows thereafter: Section 2.2 provides an overview of international relations theory and considerations on how cyberspace affects classical security thinking. The concepts presented in that section are used for theoretical reasoning later on in this thesis. As outlined earlier, this thesis is a cybersecurity or computer science thesis in an interdisciplinary setting: It applies methods from the social sciences. The concepts and theories from international relations presented in this chapter are seen as tools in order to understand neutrality and cyberspace and set these two terms into a context. The thesis is deliberately not set in a specific theoretical tradition of international relations or political science: From an engineering and computer science perspective, the theoretical traditions in international relations studies may appear as restricting a researcher to a certain theoretical stream of thinking, such as *realism* or *liberalism*. Discussions juxtaposing different streams of thinking, which are usually found in international relations theses, are omitted.

These considerations are complemented by the considerations in Section 2.3: This section provides a primer on the functioning of the Internet and further computer science related contents relevant to understanding the nature of cyberspace. The goal is not to provide a highly detailed technical description of the Internet and cyberspace

but to abstract basic principles of the functioning of these technologies, in order to enable reasoning on this basis. This section is concerned with *generation of theory* in the sense of “analytical theory and concept development” outlined in Chapter 1.

2.1 Switzerland and Neutrality

Switzerland¹, officially in full the *Swiss Confederation*, is a federal state in central-western Europe. It is located in the geostrategically interesting key area of the Alps, which forms a natural obstacle for travel between north and south. It has been a political entity for over several hundred years but has only become a proper *state* following the Napoleonic occupation. It was declared a neutral territory by the Vienna Congress in 1815, following the Napoleonic wars.

In its modern form as a federal state, Switzerland exists as the result of a civil war, which took place in 1847 and 1848, between its conservative cantons, mostly catholic and in favour of a looser federation of states, and liberal cantons, mostly protestant and in favour of a federal state with centralised ministries and an administration of its own. The liberal cantons prevailed, and so the federal state of modern Switzerland was established in 1848, and the first federal constitution was proclaimed. Although the constitution has since been amended several times, the basic principles and ideas of how the modern Swiss state works are still largely based on this original constitution.

Neutrality has always been an inherent part of the identity of the modern Swiss state: It was “inherited” in 1848 by the modern Swiss state from the aforementioned Vienna Congress declaration of neutrality imposed onto the Old Swiss Confederacy in 1815. It is not surprising that neutrality is mentioned in several articles of the Swiss constitution, as is later discussed in Chapter 4. Also nowadays, neutrality still plays a vital role for Switzerland both internally (with respect to inner politics and an element of identity for the people of Switzerland) as well as externally (as an important factor governing foreign and security policy decisions of the government). This is exemplified by a government publication from 2022 [33], which explains how Switzerland works to the broader public. Neutrality takes a prominent position: On the first page outlining some facts about Switzerland, the publication states “[Swiss] *neutrality is recognised by all states of the world.*” Further, the publication states: “*Switzerland is a neutral state: it may not take part in armed conflicts or enter into*

¹The information in the introductory paragraph is commonplace knowledge, which may be found, for example, in a 2023 article by Egli in the Encyclopedia Britannica [31, 32] as consulted in 2023, in a history book on Switzerland by Georg Kreis published in 2014 [17], or in an official government publication from 2022 aimed at explaining Switzerland’s specifics to the broader public [33].

military alliances. Switzerland’s neutrality is recognised worldwide. That is why it is often asked to mediate in conflicts or exercise protective power mandates.”

As mentioned above, Switzerland and neutrality seem to be inevitably tied together; examining one does not work without considering the other. Therefore, this section also outlines some basic knowledge about Switzerland, in order to provide the reader with sufficient context for understanding neutrality. Subsection 2.1.1 provides a very short summary of how Switzerland works. This is essential, in order to better understand the case studies in Chapters 4 and 5. Thereafter, Subsection 2.1.2 introduces some publications of the Swiss government on neutrality and discusses, why these are only of limited use for the understanding of neutrality. Subsection 2.1.3 discusses some academic literature on neutrality or, rather, the challenge of finding sufficient systematic literature on the topic of neutrality.

2.1.1 Swiss Politics

As outlined previously, a Swiss government publication from 2022 [33] provides essential details about the functioning of Switzerland as a country and historical statements may be found in common history books on Switzerland, such as in a book from 2014 edited by Georg Kreis [17]. The content in this subsection is derived from these two publications.

Switzerland consists of 26 federal entities, which are commonly known as “cantons” and are similar to federal states in the USA: Each canton has a constitution of its own, and cantonal administrative structures may differ, although there is a tendency among the cantons to harmonise structures and processes to a certain extent. A distinguishing feature of Switzerland is that it has a political system it refers to as “direct democracy” with regular referenda, as is outlined in the aforementioned government publication [33]: *“The Swiss are world champions at voting: they vote on every amendment to the Constitution. By launching a popular initiative or calling for a referendum, citizens can demand that a vote be held on a political issue.”*

The government publication also states the four national languages [33]: *“The four national languages are German, French, Italian and Romansh. 62 per cent of the population primarily speak (Swiss-)German, 23 per cent French, 8 per cent Italian and 0.5 per cent Romansh.”* Membership of a language group may have a similar character to ethnicity.

All three facts mentioned: the strong federalisation into (historic) states, the very unique political tradition of semi-direct democracy, and the diversity in terms of languages might have helped foster a foreign policy of neutrality, in order to maintain

an internal balance. As explained in Chapter 4, at times neutrality was necessary for enabling a sense of national cohesion (and, therefore, in terms of national security for the coherence of the federal state).

As the case studies conducted in this thesis often refer to specific roles in the Swiss government or in departments of the federal administration, the structure of the government, parliament, and the departments are quickly explained on the basis of the Swiss government publication already mentioned [33].

The Swiss government—called *Federal Council*—consists of seven individually elected members—*Federal Councillors*—, who have roles similar to ministers in other countries and, in fact, they may often even be commonly referred to as ministers of government. Switzerland does not have a prime minister, but one of the seven members of government is formally the head of state and is called *Federal President* or simply referred to as president. The president does not have any particular political powers or rights different to those of a federal councillor, the function is purely representative and administrative (the president heads meetings of the Federal Council).

Decisions are made collectively by the Federal Council, if required by means of a majority vote among the seven Federal Councillors. However, different to many other countries, once the Federal Council has come to a decision, every member needs to represent and support that decision in public, regardless of the personal opinion of the respective Federal Councillor. The Federal Councillors are (re-)elected by the parliament (formally the body of election is named the *United Federal Assembly*, as outlined later) every four years. Once elected, Federal Councillors cannot be impeached by the parliament until the next re-election. Federal Councillors tend to be elected from the largest political parties according to a distribution key based on customary law, however, this is not a formal rule. Hence, large left-wing, right-wing and politically centrist parties all have members in the government. However, these parties do not have a formal coalition agreement with one another. As already outlined, the Federal Council determines its political position on a case-by-case basis by means of a majority vote. The parliament scrutinises decisions of the Federal Council and often overrules these, since the majorities in the parliamentary chambers (also here on a case-by-case basis) may work differently from those in the Federal Council.

Switzerland has two parliamentary chambers: The *National Council* (consisting of 200 members), which represents the voting populus proportionally, and the smaller *Council of Estates* (consisting of 46 members), where each canton is represented with two seats, except for six cantons, which only have one seat each for historical

reasons and used to be referred to as *half* cantons. The parliamentary chambers are united together to form the *United Federal Assembly*, which elects the members of government.

As already outlined, the Federal Councillors are comparable in their role to ministers. Therefore, each of them heads the equivalent of a ministry, which is usually referred to as a *department* in Switzerland. The seven federal departments (i.e., ministries), including their respective official abbreviations, are:

- *Federal Department of Foreign Affairs* (**FDFA**);
- *Federal Department of Home Affairs* (**FDHA**);
- *Federal Department of Justice and Police* (**FDJP**);
- *Federal Department of Defence, Civil Protection and Sport* (**DDPS**);
- *Federal Department of Finance* (**FDF**);
- *Federal Department of Economic Affairs, Education and Research* (**EAER**);
- *Federal Department of the Environment, Transport, Energy and Communications* (**DETEC**).

A further entity, the *Federal Chancellery* (**FCh**), also attends government meetings but may not cast any votes.

For the purpose of this thesis, the FDFA and DDPS are most relevant, as the case studies in Chapters 4 and 5 will often refer to material or statements released by these departments.

While Switzerland is not part of any military alliances, it participates in the *Partnership for Peace* (PfP) initiative², which is affiliated with NATO. Membership in PfP is open to most countries and Russia also joined it in the 1990s, which may be a reason why Switzerland did consider joining PfP a problem with respect to its policy of permanent neutrality.

Furthermore, Switzerland, by virtue of its neutral status, hosts one of the laboratories accredited by the UN for NBC disarmament and analyses: The NBC laboratory in Spiez provides forensic and further services to the international community when requested.³

²See <https://www.pfp.admin.ch/>

³See <https://www.spiezlab.admin.ch/en/ls.html>

2.1.2 Swiss Neutrality, as seen by the Swiss Government

As previously outlined, this subsection provides a perspective on neutrality, which is shaped by official government publications of the Swiss Confederation. While these publications do not provide a particular in-depth view into what neutrality is, they still provide a first understanding of what neutrality is. While it could be assumed that, since neutrality is a central concept for Switzerland, there are documents that cover the idea of neutrality in-depth, this is not the case. As is later outlined in Chapters 3 and 4, neutrality has developed over time and is norms-based; i.e., it is not systematically defined or conceptualised. One of the reasons might be that this grants the greatest amount of freedom to the Swiss government in terms of deciding how to implement neutrality with respect to international and internal developments. Since neutrality is a central concept for Switzerland, it is mentioned in various publicly available documents, such as brochures or leaflets that inform the public. There is, however, no fact sheet or in-depth description available from the government that would cover neutrality, which is also one of the main motivations for the in-depth analyses provided in this thesis. However, some of the government brochures or leaflets that cover neutrality provide information on how the government intends to understand neutrality and a foundation for discussion, reflection, and understanding in this thesis. While it might seem unconventional, it is useful to consult these brochures, as they are the few official sources available for understanding the government's viewpoint on neutrality. As is outlined later on in Chapter 4, the debate on what neutrality is and how it should be implemented has become more heated since the beginning of the 21st century, which explains why some of the sources might seem older than would intuitively seem reasonable. These are discussed in the following.

In a leaflet released in June 2000, the Swiss Department of Defence (DDPS) presents its view on the history of Swiss neutrality [34]. The leaflet has been updated and the 4th and most recent edition was published in October 2004 [35]. These leaflets, as also a website text of the Swiss Foreign Affairs Department (FDFA) [36] from 2017, follow a similar narrative: They market Swiss neutrality as an inherent element of Swiss history and identity, upon which contemporary foreign policy is based. Equally, the publications remain very unspecific on how Switzerland might or might not participate in international conflicts and sanctions. The aim seems to be to not limit Switzerland's options of response in case of a future conflict.

The 2004 leaflet identifies the following elements that shape Switzerland's neutrality:

1. Switzerland's tradition and history of neutrality;
2. the international law on neutrality;
3. the global situation (e.g. the Second World War or the Cold War).

According to this listing, neutrality is made up of two essential factors: a legal definition and shaping of the term through the tradition of state practice and history—both are treated later as aspects of the case studies in Chapters 3 and 4. Furthermore, international politics (or: the global situation) is identified as an essential factor influencing the implementation of neutrality. The case studies in Chapter 4 will indeed indicate that global factors are an essential element influencing the balancing of any contemporary implementation of neutrality policy.

The leaflet further explains the history and emergence of neutrality, starting with the Marignano Defeat (1515) and ending with the most recent example at the time, the War on Iraq. It quotes the Swiss Foreign Policy Report of the year 2000:

“for this reason security through cooperation forms the leitmotif of the new Swiss security policy. It is against this backdrop that the Federal Council continued to pursue the strategy already presented in the 1993 neutrality report⁴ and reaffirmed in the Security Policy 2000 Report. Basic retention of neutrality coupled with the consistent use of any scope of action is an appropriate means for making a useful contribution to security and peace in the world.”

The excerpt above indicates that neutrality is seen not only as a passive strategy for staying out of foreign conflicts. Rather, it is also perceived as a tool of foreign policy, which may contribute to building and maintaining international peace. With respect to the research question of this thesis, this supports the conjecture that neutrality contributes to international stability.

The leaflet further justifies Switzerland's membership in NATO's *Partnership for Peace* programme and the UN. It justifies participation in these international initiatives by means of referring to international neutrality law, which does not restrict a neutral country from participating in such organisations. However, as explained later on, Swiss neutrality is far from purely being defined through the international law codification of neutrality. As was also outlined in a publication by the Swiss government

⁴This neutrality report is to some extent similar to a political agenda of the government in matters that might affect neutrality at the time it was written and, to another extent, mainly a more extensive version of the newer documents discussed here. For this reason, a more thorough discussion of this report is omitted, as it would not provide essential additional insights.

presented earlier in this subsection, neutrality also depends on a historic-traditional component.

It is useful to mention some drawbacks of the discussed government leaflets: Their explanations of neutrality policy need to be read with caution; the main aim seems to be to not confine any potential future courses of action. While the documents speak of a history and tradition of neutrality policy beyond the narrow definition in international law, they avoid defining what neutrality means in these terms and remain generally quite vague. They do, however, provide the insight that neutrality is shaped by two aspects: an international law codification of its principles and a historic-traditional (i.e., norms-based) approach. It is further strongly influenced by international events and, therefore needs to be analysed and investigated with respect to international events. These insights and understandings are further developed in Chapters 3 and 4.

2.1.3 Neutrality Literature

The previous subsections provide a foundation for the understanding of neutrality and the core case example country, Switzerland. Furthermore, some limitations of government publications have been explained. This subsection further elaborates on understanding neutrality by providing a short overview of the most relevant academic literature on the topic. In particular, the focus and limitations of this literature are discussed briefly; where appropriate a more thorough discussion is provided in Chapters 3 and 4.

Even though neutrality is a topic that is highly important to Switzerland, its history, and its national identity, only a limited amount of publications are concerned with what neutrality actually is. Most of these publications have emerged from Swiss authors. Over the period of researching and writing this thesis, mainly academic literature with either a historical or a legal focus has been found. Further literature, which mainly contains the opinions of individuals, exists. However, as it is not of an academic nature, it is not discussed here; This literature is, however, used as an important source for the case study on the understanding of neutrality later in Chapter 4.

A particularly important and interesting source is Alex Spring's PhD thesis from 2014 on *The International Law Concept of Neutrality in the 21st Century* [12]. It bears the perspective of a legal scholar on the topic. Nevertheless, it provides additional insights beyond a formalistic analysis of the international law sources on neutrality. First and foremost, it acknowledges the distinction of a purely legal component—in

the sense of a codification of neutrality in international law—and a component shaped by history. Spring provides the terms of *relative* and *permanent* neutrality already presented in Chapter 1. Relative neutrality denotes the international law definition of neutrality, which covers the rights and duties of a neutral state in case of an armed conflict between third parties, while permanent neutrality denotes the definition of neutrality by means of tradition and history. The latter is not necessarily a term invented by Spring; it is commonly used as a term in Swiss politics in order to refer to the Swiss model of neutrality, which is permanent. Spring provides a thorough analysis of neutrality from a legal perspective and with respect to problems of the early 21st century, such as in relation to the UN, NATO, and the EU. Many of his points are very specific discussions, which are of interest to legal scholars but less so to understanding the nature of neutrality more generally. However, he does provide some interesting considerations, which are referenced in later chapters. He provides a very short discussion on cyberspace, which, however, only constitutes that the matter is difficult with respect to cyberspace due to missing definitions of attacks in cyberspace etc. This is where the next publication is of interest, which focuses on the impacts of the cyberrevolution on international law:

The Tallinn Manuals [27, 28] published in 2013 and 2017 by the NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn (Estonia) are the outcome of an initiative that aims to define how the member states of NATO and its Partnership for Peace (PfP) interpret international law in cyberspace. The Tallinn Manuals' interpretation of neutrality law is analysed and discussed thoroughly in Chapter 3. The respective chapter underlines the Tallinn Manuals' limitations with respect to neutrality: They do not cover the aspects that are particularly relevant for neutrality due to the novel characteristics of cyberspace. Where aspects of neutrality in cyberspace are covered, the reasoning appears strange and—as outlined later on—not plausible with respect to international law and rather shaped by the national interests of the USA.

As mentioned earlier, a second group of literature exists, which provides analyses of neutrality from a historical perspective. Works, such as those by Suter (1998) [37], Hettling (1998) [38] or Riklin (1991) [5] provide very interesting case examples and analyses of Switzerland's history. However, they fail to provide an extensive and coherent theory of what neutrality is and how it is influenced by external and internal events in a systematic way. An explanation may be that a field this thesis refers to as *neutrality theory* has never been established. Most work by historians analyses neutrality at a certain time, without broader reflection on neutrality as a concept *per*

se. The historians whose work on (aspects of) neutrality is discussed in this thesis mostly emerge from Switzerland—historians from abroad have not been found to cover neutrality in sufficient detail to be relevant for this thesis. It may be assumed that the Swiss historians whose work is discussed in this thesis implicitly took the concept of neutrality for granted, i.e., they did not consider a thorough questioning of what neutrality actually is to be relevant. Moreover, as historians, they approached neutrality as defined by the respective foreign policy activities of Switzerland in the respective era covered by their work.

Riklin [5] does provide a starting point for such a *neutrality theory* by defining functions and dimensions of neutrality. However, they are far from a thorough theory on neutrality and none of the literature discovered provides a stringent taxonomy of terms that would include definitions and basic principles. Hence, the case study in Chapter 4 contributes significantly to developing such a theory of neutrality.

The literature is complemented by reports released by ETH: Notably, its regularly published neutrality report⁵ is mainly a large-scale survey of the perception of neutrality by the Swiss population. The report from 2022 [39] provides a source considered in later chapters. A further report by ETH (Cordery et al, in 2021 [40]) attempts to provide a more systematic overview of what neutrality is but mainly focuses on the legal dimension and, therefore, misses many points made in this thesis. It provides a useful short synthesis of neutrality law and some neutrality terms. It also references some of the work of this thesis, namely a paper *On Neutrality and Cyber Defence* published by the author of this thesis in 2019 at the *European Conference on Cyber Warfare and Security*. Furthermore, the author of this thesis presented his work at ETH while writing this thesis, and some of the findings in the report might have been influenced by this presentation.

Martin Dahinden, a Swiss retired diplomat now affiliated with ICT4Peace in Geneva and the University of Zurich, released a discussion paper in 2021 addressing *Swiss neutrality in the age of cyber warfare* [41]. The paper provides a very short presentation of some aspects of Swiss neutrality and cybersecurity. However, it lacks depth and should rather be understood as food for thought on the problems of modern-day neutrality. The paper drafts some of the challenges that are also outlined in this thesis: The differentiation between CND, CNA, and CNE and the challenges this poses is an example. The style of the discussion paper is that of a policy summary for high-level decision makers: It raises awareness that neutrality on the background of the cyberrevolution is challenged as a concept and deserves attention—in this sense,

⁵This thesis relies mainly on the neutrality report released in 2022 [39])

it supports the motivation for this thesis and underlines that the research conducted in this thesis is necessary. It summarises some aspects of international law with respect to neutrality. However, the discussion paper fails to thoroughly analyse the legal situation on the basis of technological givens, as is done in this thesis, and also fails to provide solutions or a critical review of discussions in the legal domain. The Tallinn Manual is referenced but its content is taken into consideration without any scrutiny or critical discussion. The paper does provide some interesting contributions in terms of the role and initiatives Switzerland could engage in with respect to its tradition of good services (see Chapter 4). One of Dahinden’s suggestions is to support fact-finding missions of international organisations, such as FIRST, financially and to establish Geneva as a centre for global governance of questions arising from international cybersecurity discussions. Furthermore, he suggests to further engage in confidence-building and norms-building measures, for example in the UN, and to support strengthening international law, as is already done by Switzerland nowadays. He also suggests that Switzerland should engage in cybersecurity capacity-building initiatives in order to improve cybersecurity capabilities globally and thus improve global cybersecurity. Some of these topics have also been found during the research for this thesis, independently from Dahinden’s publication when investigating the potential scope of neutrality on the background of the cyberrevolution; they are outcomes from the case studies and discussion of examples in Chapter 5 and are discussed there.

Finally, Swiss neutrality should not be misunderstood as a policy of pacifism: While some people would connect neutrality with pacifism and a policy, which completely refrains from using weapons, this is not the case for Swiss neutrality. As an article in *Time* written by Latson in 2015 [42] explains, neutrality is not equivalent to pacifism—rather, it might contribute to international peace, but this does not mean that it completely aligns with purist pacifist ideas. As the article outlines [42], it “*is of the greatest importance that we [(the Swiss)] leave no doubt in anybody’s mind that not even the most hopeless situation will make us capitulate voluntarily, and before we can be commanded we have got to be beaten*”. This aligns with what this thesis later defines as the principle of *armed neutrality*, an inherent characteristic of permanent neutrality.

2.2 International Relations Studies Concepts

The aim of this section is to provide an overview of international relations studies (IR) concepts relevant to this thesis. Subsection 2.2.1 introduces some terms from IR,

which are of relevance to this thesis. Thereafter, Subsection 2.2.2 discusses some work from IR, which specifically addresses the problem of cyberspace. As a general note, it is useful to mention that most international relations literature does not grant neutrality any particular importance for the conceptualisation of international relations and global politics. The central argument of this thesis, however, attempts to alter this understanding. Only a small number of countries define themselves as neutral in 2022,⁶ which may be a reason why the concept is neglected by most international relations scholars or only treated in a very minimal manner. The most commonly found theoretical conception of neutrality is with reference to the island of Melos, as has already been introduced in Chapter 1, or that of neutrality with its very narrow definition in international law and the unsuccessful example of Belgium during the World Wars. Switzerland’s success is rarely discussed or it is limited by focusing on Switzerland’s banking sector. This neglect of neutrality in the international relations literature and in the schools of thought of IR provides one of the fundamental motivations for this thesis.

2.2.1 International Relations Terms and Concepts

This thesis does not provide a thorough theoretical discussion of IR theory due to its disciplinary setting in computer science. Rather, concepts of IR that might be useful for discussions are briefly introduced, similar to an engineer defining tools and theories he relies upon in order to build newer and more advanced machines.

For an introduction to common schools of thought in IR theory, see Box 1. It provides an impression of common reflections in IR theory. Neither theory is preferred over the other and no excessive ideological debate, as is commonly found in IR theses, is provided. The theories of IR are seen as complementary and as tools for explanation and understanding.⁷

Some terms from IR, which are useful for considerations on neutrality, are introduced in the upcoming paragraph.

⁶See Alexander Spring’s discussion on neutral countries and whether they are truly neutral in the traditional sense or why they have given up neutrality in his PhD thesis [12]. His considerations are complemented by Sweden and Finland having voiced their intention to join NATO in 2022.

⁷Similar to the natural sciences, where sometimes multiple theories exist to explain the same entity of physics. This is, for example, the case with the properties of light, which may be explained through a particle model and a model relying on wave theory. Physicists usually do not have problems with acknowledging that both theories deserve respect and that different situations might yield one model more suitable than the other.

Box 1: Schools of Thought in International Relations (IR)

For a comprehensive text on the schools of thought in IR, the reader is referred to established IR textbooks, such as those provided by Nye (2017) [18] and Heywood (2014) [19]. Both textbooks outline realism and liberalism as two significant schools of thought in IR; Nye also adds constructivism.

As Heywood outlines, Realism is a theory of “*power politics*” with key themes, such as “*state egoism and conflict, statecraft and the national interest, international anarchy and its implications, polarity, stability, and the balance of power*”.^a Particularly the latter is a concept also relevant to neutrality. Liberalism, on the other hand, is seen as a theory based on an ideal of “*universal and perpetual peace*”, with the following central themes:^b “*harmony or balance amongst competing interests [...] a natural equilibrium will tend to assert itself.*” With respect to neutrality, both these theories may be useful: integral neutrality might be more applicable in an environment where the realist view dominates, while the good services or even active neutrality rely more on the liberalist view. This thesis assumes that all of these views bear legitimacy for explaining the dynamics of the international system of states. Nye adds that a further, constructivist, theory exists, which emphasises the importance of social constructs and processes in international politics, such as “*shared discourses, ideas, practices, norms, rules, and logics of appropriateness*” and that “*social structures [...] shape both identities and interests*”.^c Permanent neutrality may be seen as such a construct shaped by norms.

^aSee Heywood (2014) [19], pages 63–64.

^bSee Heywood (2014) [19], page 65.

^cSee Nye (2017) [18], pages 72–73.

Concepts and Terms from International Relations Theory

Nye [18] defines basic ideas of how systems of global politics can work: *imperial*, *feudal* or the *anarchic system of states*. The latter is a theoretical abstraction of the contemporary understanding of the basic entities of global politics. It is “*composed of states that are relatively cohesive but with no higher government above them*” [18]. Nye states that “*the Peace of Westphalia enshrined the **territorial sovereign state** as the dominant political unit*” [18]. For this reason, this concept is often also referred to as *Westphalian* system of states, which is the term used in this thesis. A further common term for this system is *Conventional Model*—this term is mostly used in connection with Lucas Kello’s work from 2017 on cyberspace [8]. This abstraction also provides the basis when reasoning about *conventional* neutrality.

A further relevant concept is that of *system stability* and a *balance of power*.⁸ Both describe some sort of equilibrium, which is relevant for stability. Nye reasons about the

⁸See Nye (2017) [18], pages 52–53 and 85–90.

former: “A major purpose of the international system is to safeguard the sovereignty and security of its members [...] The stronger the normative and institutional threads binding states and the denser the connections between them, the greater the stakes states have in preventing system breakdown”. So stability refers to the maintenance of the international system, with a focus on peace, also minor wars that do not cause significant disruptions to the international system are acceptable as well. Neutrality’s potential contribution to international stability, as outlined in Chapter 1 may be seen in this sense. The term *balance of power* is explained by Nye as “a more or less automatic equilibrium of power in the international system [...] states will act to prevent any one state from developing a preponderance of power”. Balance of power is an important consideration when explaining the emergence of neutrality as a policy, but also its contribution to stability.

A further term used in the upcoming reflections is that of a *hegemon*. It is derived from the term “hegemony”, which Heywood defines as follows:⁹ “*The ascendancy or domination of one element of a system over others*”. In this sense, a hegemonic state is a particularly dominant state within the Westphalian system. Contemporary examples might include the USA and China. Furthermore, Switzerland (or a neutral state in general), might uphold or encourage multilateral approaches to international politics. Heywood defines this term as follows:¹⁰ “*Multilateralism can broadly be defined as a process that coordinates behaviour among three or more countries on the basis of generalized principles of conduct [...] it most conform to [...] non-discrimination [...], indivisibility [...], and diffuse reciprocity [...]. Multilateralism may be informal, reflecting the acceptance of common norms and rules by three or more countries, but more commonly it is formal, in which case multilateralism equals institutionalism.*” Multilateral systems may be found to rely on a hegemonic power for stability purposes.

2.2.2 Cyberspace-related Concepts and Considerations

This subsection focuses on discussing work in the domain of IR, which characterises cyberspace and formulates conceptualisations and challenges therein. Some passages in this subsection bear similarities to papers published by the author of this thesis

⁹See Heywood (2014) [19], page 75.

¹⁰See Heywood (2014) [19], page 467.

in 2019 [43] and 2021 [3].¹¹ The reader is referred to Appendices A and B for a full listing of the contents of these papers.

A common concept for fostering understanding in international relations is that of analogies. An example with respect to cyberspace is that of comparing cyberspace to the (partially) unregulated situation on the oceans during the age of privateering, as has been brought forward by Egloff in 2017 [44]. However, most analogies do not provide a useful basis for reflections with respect to neutrality, as the analogies themselves lack consideration of neutral parties. A similar comparison could be drawn between cyberspace and the emergence of earlier telecommunication technology and its role with respect to power projection and global dominance, such as has been done by Hills in her works from 2002 [24] and 2007 [25].¹² Hills' considerations of global telecommunication and its regulation provide an interesting analogy with respect to globally operating technology companies, which might be useful for considerations on platform neutrality (see Chapter 6). However, also Hills' analogy does not provide for neutral actors and, therefore, no particular additional insights with respect to state or platform neutrality may be gained from it.

With respect to the effects of the emergence of cyberspace on international stability, global conflicts, and IR theory in general, the following considerations and concepts have been found to be useful:

First, the emergence of cyberspace as a relevant factor for national and global security has largely been accepted by IR scholars. However, the nature of *thinking* about cyberspace and its role in IR is part of an ongoing ideological debate:

Classical realist thinking aims at an approach where the state, in the sense of a *Leviathan*¹³, has to dominate and control cyberspace within its territorial boundaries. However, this neglects the fundamental new characteristics of cyberspace. The (conventional) theories of international relations do not adequately reflect the nature

¹¹According to common practice in computer science, parts of the contents of a thesis are usually submitted and, if successful, published at a double-blind peer-reviewed conference. The reuse of contents within the context of a DPhil thesis, as long as the work has been conducted during the time of DPhil studies, is permissible.

¹²Hills provides two publications (from 2002 and 2007) [24, 25] addressing the emergence of wired telecommunication networks in the 19th century and their developments during the 20th century. The works analyse the relationship between states and telecommunication companies with respect to markets, regulation, domestic control and foreign influence in a Mercantilistic sense. The analysis focuses on markets, the economy, and the state, as is common among International Political Economy thinkers.

¹³The commonly referred term of the *Leviathan* refers to a book by Thomas Hobbes with the same title from 1651 [45], which outlines a specific understanding of humans, society, and the role of the state. The natural state of things is described as chaos—where necessary, the Leviathan, for example in the form of a state, is required to bring order to this natural state of chaos.

of cyberspace—in particular its pervasiveness. Kello expands international relations theory in order to incorporate the *virtual weapon*, i.e., the effect of cyberoperations on the Westphalian system of states. The following considerations and reflections are all based on work by Kello from 2017 [8]: He claims the virtual weapon fundamentally disrupts this model of states as the dominant units of international relations theory. While the conventional model relies on a Clausewitzian approach to international conflict, Kello declares that he expands theory to post-Clausewitzian considerations. His analysis of the technological revolution and its influence on global conflict provides a thorough basis in order to explain the challenges to conventional neutrality policy. The conventional theories of international relations neglect the novel character of the virtual weapon.

Kello defines *third-order*, *second-order* and *first-order* technological revolutions and analyses their effect on the conventional model. The basic concepts of these revolutions are shortly outlined in the following:

Third-order technological revolution, also known as systemic disruption, refers to “*important adjustments within the sharp limits of the states system*” [8]. While the rational order of the international system is affected, the moral order is not. An example of systemic disruption is “*the replacement of one or a group of dominant states in the system by another*” [8]. The basic mechanisms of the states’ contest for power are not changed.

Second-order revolution, also known as systemic revision affects the moral order of the International System. It maintains the Conventional Model: A state or group of states repudiates the “*shared basic purposes of the units and rejects the accepted methods of achieving them, in particular restraints on the objectives and means of war*” [8]. Nevertheless, “*it leaves the system’s organising principle, or state supremacy, intact*” [8]. Examples brought forward by Kello are the emergence of Soviet communism and its idea of a world revolution on the one hand and the idea of permanently lasting peace as a founding principle of the European Union on the other side.

First-order revolution, or systems change, finally, overthrows the mechanisms of the conventional model in that it challenges the supremacy of states. Examples are alien (i.e. non-state) actors who try to dominate the actions of conventional states by means of new mechanisms of influence and power. It yields an altogether new type of international system beyond the concept of the supremacy of states.

This thesis argues that this classification of types of revolutions is essential to describe the challenges of cyberspace to neutrality policy. A consequence of the

systems change cyberspace brings about is the state of *unpeace* [8]: While nations are not formally at war with one another, their hostile activities in cyberspace do not correspond to the conventional understanding of peaceful co-existence either. A further aspect of this systems change is the *diffusion of power*: In a system where states no longer hold the supremacy of power, other actors and groups have increased means of power to influence the actions of states. As states no longer hold the monopoly of power, defence is also fragmented: private (and other) actors, which used to be subunits of states, develop their own defence mechanisms in order to secure their interests. This further erodes the supremacy of states, as large technology firms gain influence not only in the defence of their own systems but also in the balance of cyberpower. This is an interesting consideration with respect to the applicability of neutrality theory on large technology / social media companies in Chapter 6, where the idea of platform neutrality is introduced.

A particular shift in defence thinking with effect on neutrality policy is the irrelevance of territoriality and the pervasion of cyberspace into all dimensions of warfare. This aspect is partially introduced by Joseph S. Nye in his 2011 book *The Future of Power* [46] when he defines the nature of cyberpower. This problem is further discussed in Section 2.3 from a computer science perspective. However, in IR terms, cyberspace provides a shared space, which may potentially be sued for conflict or power projection, which does not (yet) have fully established rules. Even though hardware is subject to physical and geographical factors, cyberspace as an abstract space is “nowhere” and “everywhere”, which makes everything in cyberspace potentially vulnerable to attacks from anyone within this space, without conventional geographical restrictions. In his book from 2017, Nye [18] states: “*today, everyone from hackers to large corporations is developing the code and norms of the Internet partly outside the control of formal political institutions; [...] they add a layer of relations that sovereign states do not effectively control*”. This *erosion of sovereignty* is an important finding for the understanding of how neutrality can be adopted in cyberspace.

With respect to understanding a particular challenge in cyberspace, the work of Buchanan from 2017 on the *cybersecurity dilemma* [26] is a very valuable theoretical abstraction of a problem, which is useful for considerations on neutrality in this thesis in Chapter 5. Also Buchanan’s discussed tendency towards escalation of conflict in cyberspace is shown to counter-intuitively not apply in the case of Switzerland’s neutrality.

Buchanan’s cybersecurity dilemma arises from the difficulty—from the perspective of the victim—to distinguish between attack and espionage operations in cyberspace. As outlined by Buchanan [26], the cybersecurity dilemma generates a general tendency of accelerating conflicts in cyberspace and assumes an advantage for the perpetrator, which is novel when compared to conventional considerations on the *offence-defence balance*¹⁴ and arms control mechanisms. One of the factors impacting the dilemma is the implicit consensus of the international community that (conventional) intelligence operations are generally accepted as “unavoidable and mutually accepted evil” that all countries engage in. While this does not indicate that there might be no response to conventional or cyberintelligence operations, the response will usually not be of a belligerent nature, as intelligence operations that are purely aimed at the exfiltration of information are not recognised as an act of war.

With respect to cyberspace operations, a further challenge has been outlined thoroughly by Egloff in 2020 [48]: Even when a classification of an operation as belligerent or espionage is possible, an appropriate response is only advisable in terms of international law when the adversary is able to attribute the attack to a country or some other identifiable actor. As outlined by Egloff [48], states are able to attribute activities with some level of certainty. Nevertheless, publicising attributions and responding by means of diplomatic channels can pose a challenge, since the final proof is often missing or cannot be disclosed. This *attribution problem* further aggravates the challenges outlined by the cybersecurity dilemma.

To close this subsection, some foundational work is discussed, which challenges conventional IR theory on the background of the emergence of cyberspace. The work is analysed on its relevance with respect to the central question on neutrality and cyberspace. First Thomas Rid’s article *Cyber War Will Not Take Place* from 2012 [49], which is often considered a fundamental work of literature in IR theory with respect to cyberspace. Rid’s main claim is included in the title: He argues that there is no war that could be conducted purely in cyberspace. Furthermore, he characterises all operations in cyberspace as being either sabotage, espionage, or subversion. While his argument about a war “purely” in cyberspace seems plausible, his rhetoric also seems reductionist in terms of accepting the impact a cyberoperation could have. This impact could, as he admits, also be lethal and, indeed, there have

¹⁴As outlined by Glaser and Kaufmann in an article in 1998 [47] on the *offence-defence balance*, this term is used for the questions of the ratio between the resources required with respect to offence and defence operations of conventional warfare. The article claims (as is common generally in IR theory) that in conventional warfare, the defender has the advantage since the amount of resources required by an attacker is far higher in order to outbalance the effects of defensive measures.

been examples in the past where operations in cyberspace have caused death and destruction. Furthermore, his reduction of cyberoperations to sabotage, espionage, or subversion could also be applied to conventional warfare: After all, the mechanical destruction of an ammunition depot on its own may also be considered simply to be sabotage. However, his basic argument to think of cyberoperations as one of several components used in war, presumably alongside classical kinetic means, is plausible and also relevant for neutrality considerations. However, this does not mean that the use of hostile cyberoperations below the threshold of war could not be a challenge to neutrality per se.

Gartzke brings forward a similar argument in his 2013 article *The Myth of Cyberwar* [50]: His main claim is that cybermeans are most likely deployed alongside conventional means in an armed conflict. As previously stated, this is a plausible argument and has proven to be a reality in light of the Russian invasion of Ukraine. Even more, it is essential to understand what the risks and benefits of neutrality might be in this novel domain of warfare, which is in a constant state of unpeace (as outlined further above), even without conventional wars taking place.

2.3 A Computer Science Perspective on Cyberspace

The current section aims to introduce some aspects for consideration from a more technical computer science perspective. First, it is important to define how this thesis understands cyberspace.

Cyberspace evolves around the core technology of what is known as *the Internet*, including any components that are potentially able to exchange data over the Internet, such as computers or even USB sticks. It is very well possible, that in the future, the function of the Internet in cyberspace will be replaced by technologies that do not rely on TCP/IP (see Subsection 2.3.2). Cyberspace provides junctions to the physical world, i.e., with appropriate infrastructure, cyberspace may also influence events in the “real world”.

The following subsections aid in better understanding the technological components of cyberspace in a logical-abstract sense—i.e., they do not go into technological details but provide the general idea in order to explain what abstraction is used for considerations and reflections on cyberspace in this thesis.

Subsection 2.3.1 first explains the core components of the computer revolution, which existed before the Internet became what it is today. These components are

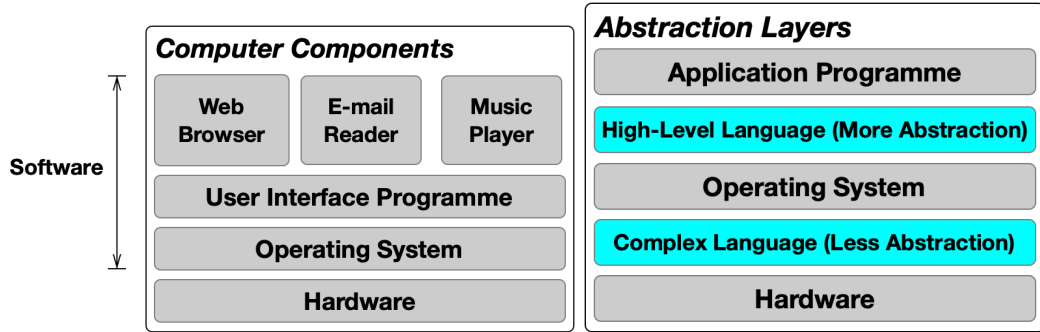


Figure 2.1: Illustrations of the conceptual components of a computer, derived from illustrations in Tanenbaum’s *Modern Operating Systems* (2014) [1], page 2 and page 5.

the computer and information or—as it is nowadays mainly referred to in its storage-enabled format—data.

Thereafter, Subsection 2.3.2 advances to what is understood to be the *Internet*.

Finally, Subsection 2.3.3 provides some general considerations on terms used in this thesis and operations in cyberspace. The subsection connects these considerations to concepts and theories on cyberspace already introduced in Section 2.2.

2.3.1 The Computer and Data

A basic conceptualisation of cyberspace has already been provided in the introductory paragraph of this section. Computers and data form an integral part of everyday life since the late 20th century and are two components which, in combination with the Internet, constitute cyberspace.

This thesis understand the computer on the basis of the idea of the *Turing Machine*: as the idea of an abstraction of a universal machine that can calculate anything intuitively defined as *computable*. The reader is referred to De Mol’s article from 2018 in the Stanford Encyclopedia of Philosophy [51] for a thorough explanation of the concept of a Turing Machine and computability, since its discussion lies beyond the scope of this thesis. It is considered a central concept for theoretical analyses in computer science and information theory. In more general terms, a Turing Machine is a machine, which can automatically calculate results—according to a programme—from inputs it is given. The limitations of what a Turing Machine can calculate are given by computability and complexity—in intuitive terms, anything that could be calculated (by hand) by means of a specific set of determined steps (even if infinite) is considered to be computable. The domain of complexity determines not only whether something

could be calculated in theory but also allows a prediction of computability *in reality*—i.e., whether a valid output can, at least with a specific certainty, be achieved within a useful amount of time. In general terms, useful applications of computing technology are problems that can be automated in a fashion that lies within a term of complexity, which is generally considered to be resolvable within a useful time—i.e., a time that a user can reasonably be expected for a result.. Typically, magnitudes of a lifetime are not considered useful, while hours, days, or even years may be considered useful.

The input and the output of a Turing Machine would generally be considered *data*. Input and Output interfaces enable the transmission of data from the *real* world into the “*cyber*”-world—or: into digital *data*.

For a more thorough understanding of how input and output in combination with the computer work, the reader is referred to Tanenbaum’s *Modern Operating Systems* in the edition published in 2014 [1].

A computer is a universal programmable Turing Machine. It usually consists of hardware—the physical components of the computer—and software—the adaptable programmes in the form of data—, including input and output systems (screens, keyboards, etc.). Illustrations of these terms may be found in Figure 2.1. The illustrations there are based on illustrations in Tanenbaum’s *Modern Operating Systems* [1] but have been made by the author of this thesis derived from the illustrations in Tanenbaum’s book due to copyright reasons. They provide a high-level abstraction of hardware and software.

As outlined previously, software is usually stored as some form of data—in this specific case the data consists of instructions that are understandable to a (potentially abstract) machine for interpretation. However, data may also represent real-world information. This thesis considers data to be an abstraction of real-world information in digital form that can be stored on a computer. The essential idea of the Internet is the ability of computers to communicate with one another and their mutual exchange of data, which is discussed in the upcoming section.

2.3.2 The Internet

The considerations in this section rely on Tanenbaum’s *Computer Networks* in the edition published in 2011 [2]. The reader is referred to this textbook for a thorough explanation of the technological foundations of the Internet.

As an abstraction, the Internet is a federated data network, or more precisely, a network of networks: Separate networks are connected to one another by means

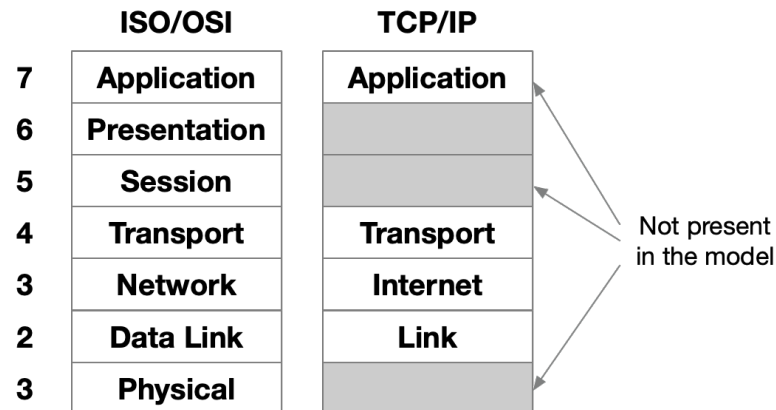


Figure 2.2: An illustration of the ISO layer model for networks, derived from an illustration in Tanenbaum’s *Computer Networks* (2011) [2], page 46.

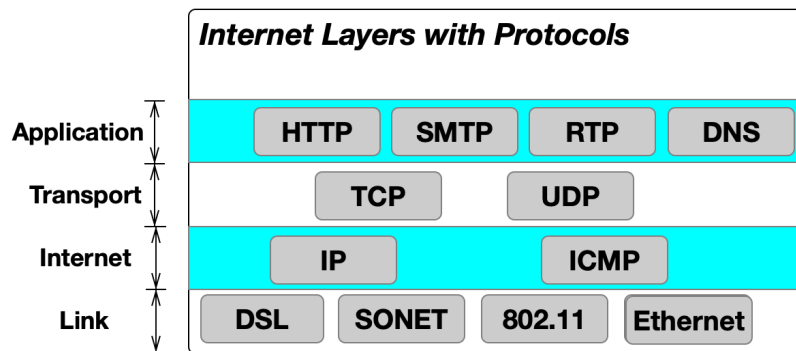


Figure 2.3: An illustration of the TCP/IP layers and common protocols used for Internet communication, derived from an illustration in Tanenbaum’s *Computer Networks* (2011) [2], page 48.

of a set of unified protocols, such as the *Internet Protocol* (IP) and the *Transport Control Protocol* (TCP), which enable the networks to communicate and exchange data. The idea of network protocols is that of a layered architecture, as is illustrated in Figure 2.2. Generally, network layers are defined by what is known as the *ISO layer* model, as shown in Figure 2.3. As a rule of thumb: the protocols further down are more concerned with physical aspects of data transmission, while the protocols further up in the layer model rely more strongly on abstract concepts and software. The physical layer might, for example, be concerned with how a bit is represented in terms of an electromagnetic signal in a cable or through radio waves.

The Internet, however, does not specify a protocol for all layers of the ISO model. Rather, it only specifies protocols for the layers shown in Figure 2.2. Figure 2.3 shows some common protocols used for Internet communication and their respective layers. Data which is sent from one computer to another over the Internet is transmitted by

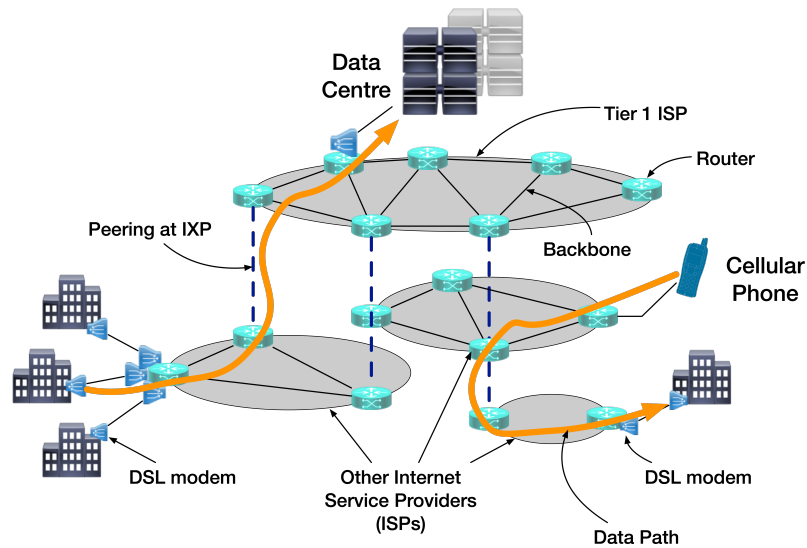


Figure 2.4: An illustration of interconnected networks, e.g., the Internet, including the aspect of routing. The graphic is derived from an illustration in Tanenbaum’s *Computer Networks* (2011) [2], page 62.

means of IP *packets*, which is related to a further important concept of the Internet: *routing*:

IP packets travel from their source to their intended destination via a *route*. Routing protocols dynamically adapt the route of a packet to be efficient on a best-effort basis: Different parts of the network may advertise the “distance” of a destination and any node in the Internet may forward packets along the route that it considers to be the most efficient. Furthermore, different networks that make up the Internet might apply different routing mechanisms with different priorities for different routes. The important conclusion is that packets with the same origin and destination may travel on different routes, depending on factors such as the routes available, the routing algorithms applied, the status of the network, etc. This provides for a very flexible structure of the Internet: Routes are dynamically chosen; if a route is no longer available but an alternative route exists from sender to destination, the data packets can still be exchanged. The fundamental idea of the Internet is that it provides a means by which any source may send packets to any destination, as long as there is a route available through a finite number of intermediate Internet nodes. Therefore, any information on a network that is connected to the Internet may, in theory, be accessed on any other network connected to the Internet more or less instantaneously. It is exactly this property, which inherently makes the Internet and cyberspace something revolutionary and completely novel: The Internet and all connected computers, as

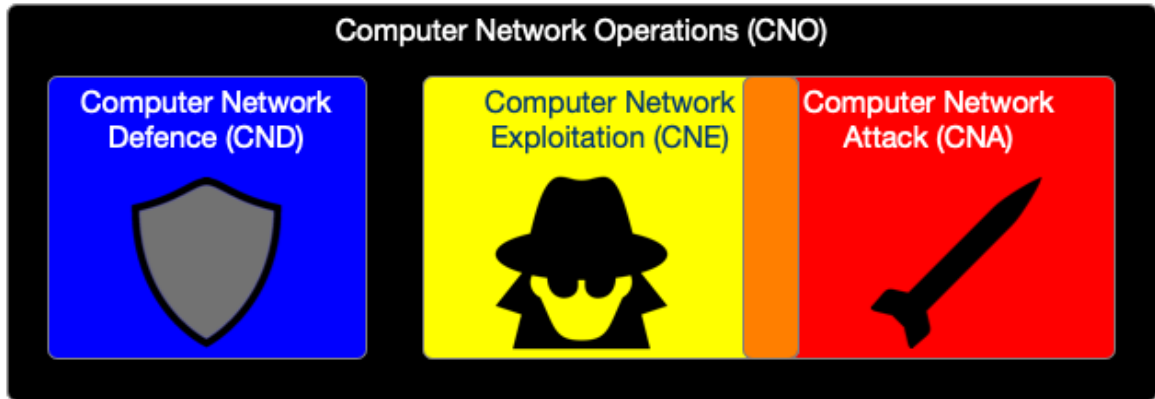


Figure 2.5: The different types of CNO: CND is defined as non-intrusive. CNE and CNA are intrusive and overlap. The graphic is taken from a paper by Stolz (2021) [3].

well as the data stored on them, become one large interconnected space, where all the content may potentially be accessed from any part of the network instantaneously: The Internet seemingly overcomes space and time and creates a virtual space inter-connecting any computer and its data, which has a connection to the Internet. This and the aspect of routing are illustrated in Figure 2.4, which is again taken from Tanenbaum’s *Computer Networks*.

2.3.3 Technological Considerations on Operations in Cyberspace

This subsection introduces some general considerations and concepts concerning operations in cyberspace, which are required in later chapters. These ideas are specific to the understanding of operations in cyberspace and to some extent related to what has already been discussed in the previous section concerning the cybersecurity dilemma. Some of the contents are reused from a paper published by the author of this thesis to an international double-blind peer-reviewed conference in 2021 [3], which is also available in Appendix B.

Operations in cyberspace usually involve the exploitation of security holes in computer systems and networks to achieve their goal. A technical, high-level conceptualisation of these operations in cyberspace is provided in the following.

Firstly, a concept common to many western military organisations is introduced. It divides (state) operations in cyberspace into subcomponents. The overall term used for operations in cyberspace on a tactical level is *Computer Network Operations* (CNO). CNOs are further divided into *Computer Network Defence* (CND), *Computer Network Exploitation* (CNE), and *Computer Network Attack* (CNA), as illustrated in Figure 2.5. This division of CNO into CND, CNE, and CNA is common in NATO

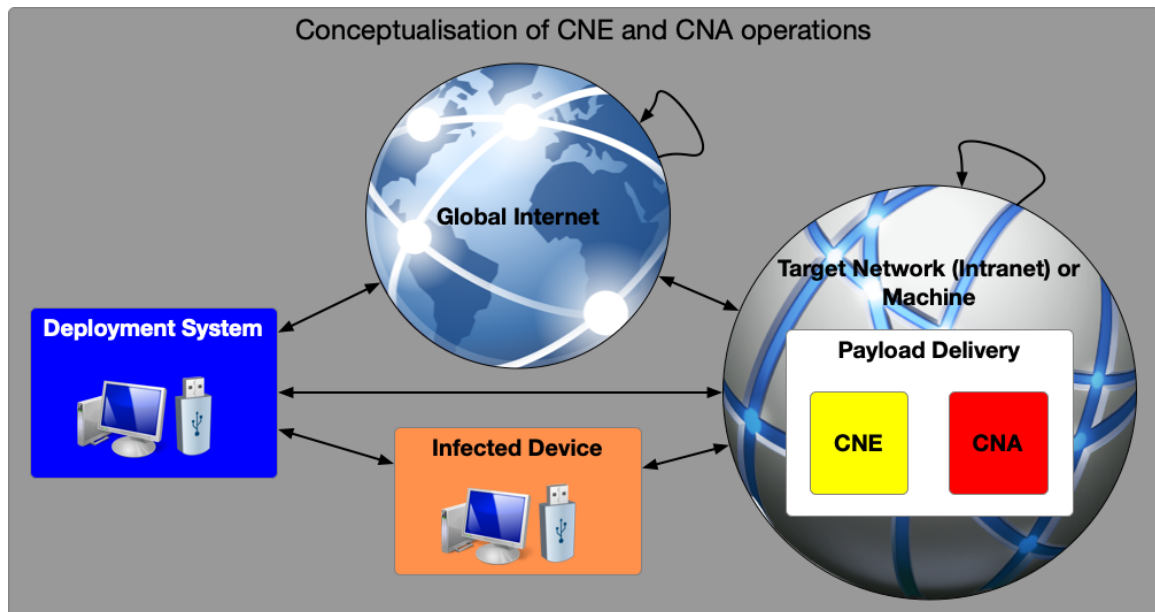


Figure 2.6: Illustration of intrusive operations in cyberspace, as published by Stolz in 2021 [3].

and some Partnership for Peace countries. For example, the Swiss Armed Forces, explain their understanding of these terms in their documents on military doctrine from 2019 [52]. Similar definitions have also been outlined by Spring in 2014 [12] based on the *US Military Strategy for Cyberspace Operations* from 2006 [53]. Spring emphasises the disruptive component of CNAs as well as their potential to destroy information in computers, networks, and connected infrastructure. He further outlines that CNE focuses on the collection of information for intelligence or reconnaissance purposes and that CNE operations do not alter the content or condition of a system: *“the infiltrated system appears the same as prior to a CNE”* (see pages 234ff [12]).

The focus of CND is to protect a party’s networks from attacks. Thi thesis pre-sumes CND does not include any intrusive measures or operations in external systems, machines, or networks. Excluding intrusive measures enables a clear distinction between CND on the one side and CNE and CNA on the other.

Both CNE and CNA affect external systems. An adversary might be interested in being able to distinguish these operations from one another in order to conduct appropriate military, intelligence, diplomatic, or other countermeasures. CNE and CNA are conceptualised based on their propagation through cyberspace and their effect on systems. An illustration of CNE and CNA operations is shown in Figure 2.6. An operation is usually deployed from a system different to machines attributable to the perpetrator in order to ensure obfuscation. This is of particular interest to intelligence

operations. Systems that deploy an operation might be USB sticks or computers that are attached to the global Internet. The most common approach is to deploy an operational asset via a deployment device on the Internet, i.e., the operational asset propagates through the Internet before reaching the adversary's network. This usually involves the arbitrary infection of intermediate devices that are not the main target, until the operational asset reaches its intended destination. A deployment system might also be specifically targeted with the knowledge that it will be connected to the adversary's network, or infect machines that are not connected to the global Internet but will be connected to the adversary's internal network or its systems; as has been the case for Stuxnet (see for example the discussion by Buchanan from 2017 [26]). Figure 2.6 includes the possibility of propagation of an operational asset through the global Internet, using an intermediary device/system or possibly also by direct connection of the deployment system to the adversary's network or machines; these appear to be the most common options from a technological perspective. The propagation of the operational asset as it has been explained applies to both CNE and CNA.

The distinction between CNE and CNA is determined by means of the effect on the target system: CNE does not appear to alter the target system, while CNA has a (destructive) impact on the target system. However, it is difficult for a victim to distinguish, whether an operation targeted against it is an attack or an espionage operation:

As illustrated in Figure 2.6, CNA and CNE are similar in terms of their propagation through cyberspace. Even as they reach their target system or network, they remain indistinguishable. Gaining access to a system or network by means of infiltration is common to both CNAs and CNEs. This does usually involve gaining control of a system. CNE and CNA differ only in terms of the payload delivery in the target system. Both exploit vulnerabilities to propagate and gain access to external systems. Once a CNE reaches its target, it applies a mechanism that allows access to sensitive information and its subsequent exfiltration. CNA, on the other hand, usually establishes a presence on the target system and afterwards delivers a (destructive) impact that will become recognisable to the opponent. However, CNAs may gain access to a system or network and then remain idle for some time before the perpetrator decides to trigger the payload.

The opponent may, using CND, be able to identify operations aimed against it. Nevertheless, the opponent might not be able to identify whether the operation was a CNE or a CNA: as stated in the documents of the Swiss Armed Forces from 2019 [52],

a CNE-like operation might function as reconnaissance in order to enable the later deployment of a CNA. The adversary could attempt to analyse the type of malware or infection used and the software it ports in order to try and identify the nature of the operation. However, this might induce significant delays in response to a discovered attack. A distinction between CNA and CNE operations is difficult for the adversary before any CNA payload is delivered and the impact is discovered.

This “indistinguishability” of CNA and CNE operations can induce problems both for the adversary and the perpetrator. While the adversary will require classification as either CNE or CNA in order to decide on adequate response measures, the perpetrator could be confronted with the accusation of having deployed a CNA operation while actually having deployed a CNE operation. As such, the indistinguishability could accelerate conflicts due to an alleged belligerent nature attributed to an operation. On the other hand, a conservative response by the adversary bears the risk of classifying an actual CNA operation as CNE and can result in a significant disadvantage. As outlined in Section 2.2, this problem has been explained in terms of IR theory by Buchanan in 2017 [26] as the *cybersecurity dilemma*— with a general tendency of accelerating conflicts in cyberspace and an advantage for the perpetrator.

Finally, terms relevant for understanding content in subsequent chapters are explained in the following:

- **zero-day** or *Advanced Persistent Threat (APT)*: Zero-days are system vulnerabilities which are not yet known to the general public. As a consequence, they are very difficult to discover and when deployed, are referred to as an APT;
- **backbone network**: The backbone network may be understood as quite literally a backbone of a network: it provides large-bandwidth high-speed connectivity, connecting several network provides together;
- **“hack back”**: This term refers to a CNA or CNE, which is deployed by the victim of a CNA or CNE, in order to investigate the origins the CNA or CNE suffered. It always happens in response to a CNA or CNE suffered.

Chapter 3

Neutrality as Defined in International Law

As outlined in Chapters 1 and 2, neutrality is a concept that is also defined in international law. In order to understand and define the conventional concept of state neutrality, this chapter explains the legal definition of neutrality. While the concept of neutrality is further defined by means of a state's (foreign) policy decisions in the sense of norms and customary law, this chapter focuses on the legal definition of neutrality in the sense of codified international law.

Chapter 4 will outline a historic approach to defining neutrality, which is synthesised with the contents of this chapter in Chapter 5, in order to gain a thorough and broad understanding of conventional neutrality policy.

The concept of neutrality has been applied to states as far back as in ancient times (see Chapter 1), yet it has only been codified in international law since 1907: Neutrality is defined in The Hague Conventions of 1907 [54, 55]. The conventions cover neutral powers and persons in war on land in *Document V* [54] and neutral powers in naval war in *Document XIII* [55]. These documents define actions and restrictions that neutral powers are bound to during times of conflict. They are specific to the (kinetic) warfare of their time—and, therefore, fundamentally different to most conflicts in cyberspace the world has seen so far.¹ Their approach towards war is territorial or geopolitical. The Hague Conventions of 1907 assume a clear area of land or sea that is controlled by a neutral power. While the legal codification of neutrality from 1907 is still valid, it might not consider the specifics of cyberspace.

In the following, the content of The Hague Conventions is presented in Section 3.1. There have also been some reflections on how international law concepts translate to

¹See also Chapter 2 and the work by Kello [8] and Buchanan [26] (both published in 2017) for further details.

challenges in cyberspace. This work is discussed in Section 3.2. The publications covered in that section are the *Tallinn Manuals*. Thereafter, some further academic work that addresses the situation of neutrality in international law on the background of the emergence of cyberspace is discussed in Section 3.3. Finally, some preliminary conclusions are presented—in the sense of analytical theory and concept development—in Section 3.4.

3.1 The Hague Conventions of 1907

This subsection presents and reflects the contents of The Hague Conventions of 1907 [54, 55] with respect to neutrality². It defines the rights and duties of a neutral country with respect to “belligerent” powers, i.e., with respect to countries that are at war with one another. Therefore, a neutral country is a third party that chooses not to participate in a war between other countries. Since a third party could support belligerents even when not participating directly in a conflict, for example by providing resources to one of the belligerents, the international law defines “rights and duties” of neutral countries, as is evident from the titles of the respective documents of The Hague Conventions of 1907: Document V [54] is labelled *The Rights and Duties of Neutral Powers in Case of War on Land* and Document XIII [55] is labelled *The Rights and Duties of Neutral Powers in Naval War*. In the following paragraphs, some key points defined in the two documents are discussed, including short reflections on potential consequences with respect to cyberspace.

3.1.1 General Obligations of a Neutral Party

The Hague Conventions generally define that a neutral power must avoid any action that would yield a significant advantage to any of the belligerent powers. Furthermore, it must restrict belligerent forces to pass through its territory. This rule is slightly less strict on sea, where passing is allowed under some circumstances. Belligerents are forbidden to move troops or convoys through a neutral country’s territory, as is defined in Article 2 of Document V [54]. Furthermore, corps of combatants may not

²Some aspects of neutrality law are also covered in the Geneva Conventions [56–62] from 1949, 1977, and 2005. However, the Geneva Conventions focus rather on the rights of civilians and third parties that are usually not considered part of hostilities. They outline what protection these parties enjoy and define some roles that neutral powers may take. Such a role is taken, for example, by Switzerland, as host country to the *International Committee of the Red Cross* (ICRC). This thesis omits an in-depth discussion of the Geneva Conventions since the author does not consider the contents of the Geneva Conventions to be a useful advancement to the research question of this thesis.

be formed or recruited on the territory of a neutral country's territory (see Article 4 of Document V [54]). According to Article 5 of Document V [54], a neutral country *must not* allow any of the aforementioned acts on its territory.

The passing of belligerent forces through one's territory or territorial waters could be deemed relevant with respect to cyberspace, when considering the passage of IP traffic³ through networks located within a neutral country, in case the IP traffic would be considered to be similar to what is indicated by *belligerent force*. However, it is more likely that traffic alone would not be deemed to be a belligerent force, since there are articles discussed later on, which are more fitting for web traffic. On the other hand, infrastructure (i.e., a computer system) that is used to generate traffic for malevolent intent could potentially be classified as "belligerent force", troops, convoys, or a corps of combatants—therefore, abuse of such computer systems or other similar infrastructure for belligerent cybersecurity operations would be forbidden within a neutral country's territory.

3.1.2 Provision and Transition of Goods

According to Article 6 of Document XIII of The Hague Conventions of 1907 [55], a neutral power is not allowed to supply war material in its capacity as a state to any belligerent party. Nevertheless, a neutral party may allow the export and also transit of goods, including ammunition or arms⁴.

With respect to cyberspace this could be interpreted as follows: While a neutral state would not be allowed to provide software that could be used for an attack (i.e., in the sense of a "weapon"), a neutral state would not be required to restrict private companies on its territory to provide or re-sell such software (although criminal codes of most countries would probably prevent or strongly regulate the provision of such software by private companies).

3.1.3 Articles Referring to Communication Infrastructure

The Hague Conventions are clearly based on a territorial conception of conflict. Any belligerent action from neutral territory is forbidden. The documents contain a small number of articles referring to telegraphy stations and telephone lines, which could

³See Chapter 2 for an explanation of what IP traffic is, how routing works, and this thesis' conceptualisation and definition of cybersecurity operations/CNO.

⁴See Article 7 in Document XIII of The Hague Conventions of 1907 [55] and Article 7 in Document V of The Hague Conventions of 1907 [54].

indicate a direction for the application of neutrality law in cyberspace since the Internet to some extent evolved on the basis of telephone networks⁵. The articles are shortly discussed in the following.

Document XIII of The Hague Conventions of 1907 [55] states in its Article 5 that:

“Belligerents are forbidden [...] to erect wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land and sea” [on the neutral power’s territory]

Document V of The Hague Conventions of 1907 [54] is more specific, with several articles covering similar arrangements. Article 3 states that belligerents are forbidden to:

1. *Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;*
2. *Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.*

Thereafter, Article 5 states that a neutral power must not allow any of the acts referred to in Article 3 on its own territory.

Article 8 adds a more detailed specification on what is and what is not allowed with regard to communication infrastructure in a neutral powers’ territory:

“A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to Companies or private individuals.”

The articles are very clear on purely military communication infrastructure: It is forbidden for use by belligerents when located on a neutral party’s territory and also the neutral party is obliged to ensure this. The stated articles do, however, allow communication infrastructure, which is not *“for purely military purpose”*; in particular, a neutral party does not need to restrict the use of civilian communication infrastructure that might also be used by the belligerents. While some articles refer

⁵See explanations in Chapter 2 and the works by Hills from 2002 and 2007 [24, 25].

to *wireless* and others to wired installations, the overall provisions follow the patterns just described, regardless of the type of communication infrastructure.

This may be translated to cyberspace as follows: Any Internet infrastructure, which is used for passing traffic, does not need to be restricted for use, as long as it is civilian infrastructure (e.g., Internet backbone connections and private civilian or public networks⁶). Therefore, a neutral party must not take any steps in terms of controlling web traffic that passes through its territory, as long as no solely military infrastructure is present that could be used by one of the belligerents.

3.1.4 Rights of Neutral Parties

Neutral parties are protected by means of the law on neutrality according to the documents listed previously. This protection is presumably one of the major motivations for countries to declare their neutrality with respect to a conflict. Belligerents are not allowed to violate the territory of a neutral party⁷, or to move any military convoys or troops through the territory of a neutral party⁸. Furthermore, neutral parties have the right to protect themselves from violations of neutrality, even by force, without this being considered a “*hostile act*”⁹. In general, neutral parties may be considered entities that should be safe from hostile activities carried out in a conflict by third parties, and a neutral party is even permitted the use of force in case its neutrality is violated without this being considered a hostile act. This can be considered to explicitly allow a neutral country to conduct CNO in order to restrict and close down any CNO targeting systems on its territory—even if this includes gaining control of systems in foreign countries by means of malware or unauthorised access (commonly known as “hack back”, as outlined in Chapter 2). Furthermore, neutral parties are only expected to enforce the law of neutrality within their own territory, e.g., a neutral party is not expected to invade another country in case that country has at some point violated its neutrality.

With respect to cyberspace, this leads to the following conclusions:

- A neutral party should not be impacted by hostile activities between third parties in cyberspace, i.e., infrastructure, networks, servers, etc. within its territory should not become affected by belligerent activities:

⁶See Figure 2.4 in Chapter 2 for an illustration of backbone networks.

⁷See Article 1 of Document V of The Hague Conventions of 1907 [54].

⁸See Article 2 of Document V of The Hague Conventions of 1907 [54].

⁹See Article 10 of Document V of The Hague Conventions of 1907 [54] and Article 26 of Document XIII of The Hague Conventions of 1907 [55].

- a neutral party may take appropriate countermeasures in case it is being attacked by any of the belligerent parties, without this being considered a hostile act;
-

The latter point could be interpreted as follows:

A neutral party, if affected by belligerent activities of third parties, may launch a counter-attack against computers that have been used by the belligerent parties and might have impacted infrastructure, networks, or systems on the neutral party's territory.

3.1.5 What is Not Covered in International Law

While the articles, conventions, and treaties discussed above provide a legal foundation for the rights and duties of neutral countries during times of war, they do not define any rules for countries that would like to pursue neutrality permanently. Therefore, neutrality is only defined *relative*¹⁰ to a third-party conflict and not as a *permanent* concept that could be pursued also during times of peace.

Furthermore, international neutrality law focuses on territorial aspects of warfare—known as *kinetic* warfare¹¹. Since cyberspace did not exist when neutrality law was written, it is also not covered by it. Nevertheless, the concepts and ideas implied by the law may be transferred to cyberspace to some extent, as is outlined in the subsequent paragraph.

3.1.6 Application of Neutrality Law to Cyberspace

As discussed, The Hague Conventions form the foundation for the definition of neutrality in international law. However, they are restricted to conventional (kinetic) warfare, which is officially declared between state actors. Furthermore, the conventions were designed before the emergence of cyberspace and bear a conventional, territorial, and kinetic focus.

¹⁰This notion has already been introduced in Chapters 1 and 2. The analysis of the international legal documents previously discussed led to this conclusion and this was later confirmed when studying Spring's work on neutrality from 2014 [12].

¹¹This term has already been introduced in Chapter 2: *Kinetic* warfare denotes warfare by traditional means, i.e., with a territorial/geographical component and commonly studied through considerations based on the Westphalian system of states or its predecessors.

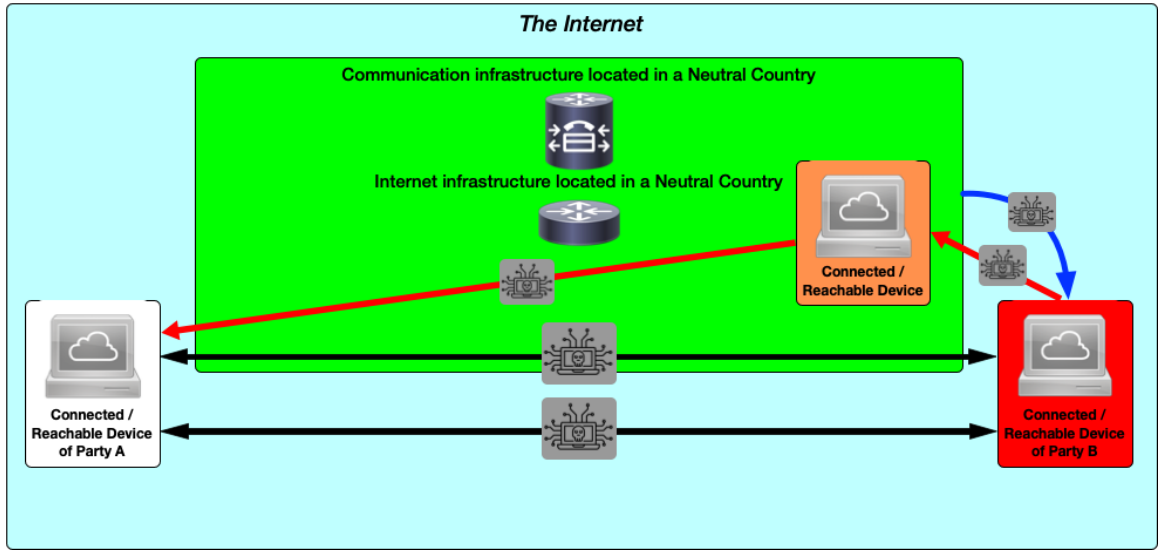


Figure 3.1: Implications of neutrality law for cyberspace.

While the law fails to address cyberspace explicitly, some deductions can be made and implications drawn for cyberspace nevertheless. These have already been discussed to some extent in the previous subsections. They are outlined in the following and illustrated in Figure 3.1.

The figure illustrates a key scenario for the application of neutrality law in cyberspace, where two belligerent parties, *Party A* and *Party B*, engage in hostilities in cyberspace: The green box denotes communication and network infrastructure (including parts of the Internet) that is physically located within the neutral party's territory. Systems located in the neutral party's territory are therefore shown within the boundaries of the green box. Systems not directly physically connected to the neutral country's networks (and, therefore, also not physically located on the territory of the neutral country) are shown outside the green box.

The belligerents, *Party A* and *Party B*, now engage in hostilities with one another, since they are in a state of war. In the illustration hostilities taking place in cyberspace are denoted by arrows. On the one hand, there might be hostilities carried out between systems of *Party A* and *Party B* which are located outside the neutral country's territory. This is illustrated by the black arrow going from *Party A* to *Party B* without passing through the green box (i.e., without passing through networks/parts of the Internet located in the neutral country). On the other hand, there is a direct arrow which does pass through the green box. As explained earlier, both of these hostile activities between the belligerents are considered to be acceptable, even if they pass through (non-military) communication infrastructure of the neutral party's territory.

This is a finding deducted from the respective articles of The Hague Conventions discussed earlier: They state that a neutral party is not called upon to prevent the use of non-military communication infrastructure on its territory, even if it is used by the belligerent parties.

The figure also illustrates cases where a belligerent—in this case Party B—attacks or gains control of a system that is physically located within the neutral country’s territory. The case where the belligerent attacks the system on the neutral party’s territory is discussed first in the following. Already the attack may be considered a breach of the neutral party’s rights since the attack has to be considered a hostile act against the neutral on its own territory. However, this case is less interesting, since the neutral country, in this case, would also become a party to a conflict between itself and Party B, in which it would by definition no longer be neutral.

In the more interesting case Party B gains access to a machine within the neutral party’s territory, in order to use that machine for hostile action against Party A. Party B may have gained access by means of force—e.g., a cyberattack, which would itself already constitute a breach of the neutral country’s rights—or non-intrusive means, such as renting systems, which can commonly be done through systems like for example *Amazon Web Services*¹². Party B would then initiate hostile action against a system of Party A, which would then be seen as carried out through a system located in a neutral country’s territory. All of these cases are denoted by a red arrow since they are not permitted under the right of neutrality.

Since the cases discussed would mean a breach of neutrality, the neutral party would be allowed to take action, including force, in order to restore its neutrality—this is denoted by the blue arrow. Specifically, this would mean that a neutral country may launch a counter-attack, in case a system on its territory has been attacked or abused for hostile actions within an armed conflict. The neutral country would not lose its neutral status under these circumstances, even though it would be conducting activities against one (or both) of the belligerents which would usually be considered hostile.

The scenario illustrated in Figure 3.1 raises one question: Why is the usage of the networks within a country’s territory for the passage of malicious traffic treated differently to the case of using systems within a neutral country’s territory to generate malicious traffic? After all, in both cases, traffic that is harmful to a belligerent party emerges from the network located on the territory of a neutral country. Should the

¹²Many other systems exist—the discussion of different types of cloud services and customers’ possibilities to specify where the services should be located lie beyond the scope of this thesis.

neutral country not be committed to restricting *any* malevolent traffic from passing through its territory, whether originating from outside its territory or within?

However, the distinction between network and computer system follows from the articles in The Hague Conventions discussed, which allow the use of communication infrastructure, which are “open to public messages” (see Articles 3 and 8 of Document V of The Hague Conventions of 1907 [54]). Being open to public messages is the inherent characteristic of the Internet: messages can be passed from a source to a destination along any route—also through Internet infrastructure on neutral territory—without the sender or receiver specifying the route (see Chapter 2 for details). A computer system, on the other hand, is not for passing messages; rather, it is used to “generate” messages or IP Traffic, which are used for an attack in cyberspace. Therefore, a computer system used by the attacker is not tolerable, when operating from a network located in a neutral country, and may be compared to a weapon system operating from a neutral country’s territory.

Furthermore, it has been found that goods and materials of a belligerent nature may be supplied by private companies within a neutral country—not, however, directly by a neutral country’s government. With respect to cyberspace, this rule might be applicable to malware or knowledge about security holes, e.g., companies selling “zero-day”¹³ vulnerabilities.

3.1.7 Conclusions for Cyberspace

From the findings in the previous subsections, this thesis concludes that neutrality law, while dating from a time before cyberspace, may be applied to scenarios in cyberspace. International law explains what rights and duties neutral parties have in a declared, conventional conflict and provides a foundation for understanding the concept of neutrality in a more abstract and general sense, from which more specific legal implementation principles may be derived, even for situations that were not yet known during the formulation of neutrality law.

A general principle of neutrality could be formulated as follows: Nothing within the territory of a neutral country should be affected or affect any of the parties of a conflict. However, the mere passage of goods, materials, or messages, even if emerging from or passing to a belligerent party, is allowed. The provision of material or goods of a belligerent nature may not be supplied directly by a government of a neutral country—nevertheless, such provisions are allowed to some extent if provided

¹³See Chapter 2 for a definition of the term *zero-day*

by private companies in neutral countries and if provided equally to either party of a conflict. This rule may be applicable to malware or other technical tools useful in conflicts. On the basis of these findings, the law has been applied to an exemplary scenario in cyberspace.

Nevertheless, the law does not cover some specifics or difficulties with respect to conflicts in cyberspace. It leaves a number of points unaddressed:

- Neutrality law only defines the neutrality of a country relative to a conflict of third parties. What happens in times of (un)peace or when there is no declared conflict?
- While neutrality law allows the deduction of principles also for cyberspace, it does not address some of the difficulties of malevolent activities in cyberspace. For example, it neglects the difficulty of attribution in cyberspace or the difficulty of distinction between CNA and CNE.¹⁴

The points listed are discussed later in this chapter.

3.2 The Tallinn Manuals

As discussed in Chapter 2, cyberspace is revolutionary in that it—seemingly—overcomes conventional territorial boundaries: By doing so it challenges conventional concepts of statehood, such as sovereignty and its territorial definition. Consequently, concepts of international law that rely on a conventional territorial understanding of states are challenged. Their applicability to cyberspace needs to be discussed and analysed, and their meaning potentially redefined or specified with respect to cyberspace. As outlined in the previous subsection, neutrality is also defined on the basis of a territorial understanding in international law and, therefore, it is affected by the challenges outlined.

The Tallinn Manuals (published in 2013 and 2017) [27, 28] are a set of rules and comments by legal scholars on the applicability of international law in cyberspace with respect to international conflict. The manuals were released by the NATO *Co-operative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn, Estonia. The manuals' contents are discussed and respective conclusions are deduced in the upcoming paragraphs.

¹⁴These problems are introduced and thoroughly discussed from an international relations perspective by Buchanan in his work from 2017 [26], where he formulates his concept of the cybersecurity dilemma. It is covered in Chapter 2 and the points raised are thoroughly discussed with respect to neutrality later on in the current chapter.

3.2.1 General Remarks on the Tallinn Manuals

The first edition of the manual was released in 2013 under the full title *Tallinn Manual on the International Law Applicable to Cyber Warfare* [27]. The second edition was released in 2017 under the full title *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* [28]. As the titles imply, the first edition focused on warfare, whereas the second edition addressed the international law situation for cyberoperations in general. The difference in terms of focus is explained in the introduction to the second edition [28]:

“The [first] Tallinn Manual’s focus was on cyber operations involving the use of force and those that occur in the context of armed conflict. Although such cyber operations will typically be more worrisome from a national security perspective than those that occur in peacetime, States have to deal with cyber issues that lie below the use of force threshold on a daily basis. Therefore, in 2013, the NATO CCDCOE launched a follow-on initiative to expand the Manual’s scope to include the public international law governing cyber operations during peacetime.”

The second edition of the manual, therefore, addresses the problem noted in the previous paragraph and introduced in Chapter 2: international law considerations only cover the case of conventional, declared armed conflicts. However, they do not address what Kello calls a state of *unpeace*¹⁵.

The introduction further outlines that the second edition “*supersedes the first*” [28] and that the original rules formulated in the first edition have been extended, altered, and further rules have been added. For this reason, if not further specified, any references to *the* Tallinn Manual in this thesis refer to the second edition [28].

As outlined in the introductions of both the first and the second editions, the documents do not represent the official view of NATO or any affiliated countries; the rules were formulated by experts from those countries, who did not represent in any way the official views of their governments. The rules passed during the Tallinn Manual process were passed on the basis of consensus. Where this was not the case, this is explicitly stated in the commentary of the respective rule. However, the rules are considered to be binding in the following sense¹⁶:

¹⁵See Chapter 2.

¹⁶See the introduction of the Tallinn Manual 2.0 [28].

“To the extent the rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors.”

This means that certain laws, even though not signed by all states, are accepted as general international practice and by means of this receive binding character.¹⁷ On the other hand, the text is described as an *“expression of the opinions of the two International Groups of Experts as to the state of the law”* in the second edition of the Tallinn Manual [28]. The rules in the manuals are, therefore, technically non-binding (since they do not represent an international treaty) but may be considered binding in the sense that they represent an expert consensus as to how international law applies with respect to cyberspace and that these experts themselves consider that these rules have been formulated on the basis of customary international law and should therefore be considered to have a binding character, even if the manuals and the rules contained therein are not binding *de iure*.

It is useful to further consider that the text, while not officially representing the view of NATO or any of its members or affiliated countries¹⁸, nevertheless has a semi-official character: It is an official publication of the NATO CCDCOE and while, as outlined, it is not a binding international treaty, it nevertheless represents the opinions and findings of a process that involved experts and stakeholders from NATO countries and its partners. It may be concluded that, while the Tallinn Manuals do not provide an explicit authority with respect to the application of international law in cyberspace, the formulated rules may nevertheless be considered normative, due to the process, stakeholders, experts and institutional affiliations that led to the publication of the Tallinn Manuals. On the other hand, this may also be seen as a reason why the rules formulated might not be considered universally valid: Even though participation in the process of formulating the rules was not restricted to NATO members (it did allow the participation of further affiliates, such as those of *Partnership for Peace*), it is centred around a specific block of countries. Different blocks of countries, centred for example around China or Russia, may hold different views. For that reason, a neutral country could also choose to not follow the Tallinn Manuals, since that could be perceived as siding with a specific block of countries.

¹⁷See elaboration on customary international law on the website of the ICRC (accessed in 2022) [63]: *“Customary international law [...] derives from ‘a general practice accepted as law’”*.

¹⁸An affiliate country could be a country that NATO collaborates with or a country that is a member of the *Partnership for Peace*¹⁹, such as Switzerland.

¹⁹See Chapter 2.

For the purpose of this thesis the Tallinn Manuals will nevertheless be considered a useful source for reflection with respect to findings from the previous section since they provide an additional perspective on the concept of neutrality. Their contents are critically reflected in the following and juxtaposed to the findings earlier in this chapter.

3.2.2 Some General Terms

It is useful to understand the Tallinn Manual’s definition of “cyber attack”, “cyber weapons”, and its approach towards espionage. These are outlined in the following, with reference to rules and corresponding commentaries where they are defined.

First, the Tallinn Manual does not elaborate on the general problem of defining what a “cyber weapon” is. The commentary of Rule 103 defines it as a “cyber means”, which is designed or used with the intent to cause physical damage or injury to people or objects. However, this neglects damage to virtual objects or *information* in cyberspace, which might, depending on the circumstances, also be of a critical nature to national security. The difficulty of defining weapons in cyberspace is outlined in detail in a PhD thesis authored by Jantje Silomon in 2021 [64]. The Tallinn Manual, when referring to a “cyber weapon”, bears a focus on cyberoperations of a purely physical notion.

Second, the term “cyberattack” is defined as follows in Rule 92:

“A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.”

Therefore, any activities that are, in their effect, restricted to cyberspace, are explicitly not considered cyberattacks; any operations involving information theft, altering of information, shutting down of systems etc. would not be considered a cyberattack, unless their impact causes damage or injury, as is outlined in the commentary of the rule.

Third, Rule 32 defines that:

“Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so. ”

The commentary outlines that only espionage operations that are carried out in an unlawful way with respect to international law would violate international law, whereas

espionage per se is generally accepted even if not favourable—in other words, espionage is considered a “necessary evil” that states generally carry out but do not favour experiencing from other states. Cyberespionage activities could, however, form part of greater operations that could be considered unlawful under international law.

From the definitions above it is evident that the Tallinn Manual bears a focus on physical effects of cyberoperations, such as operations that cause damage or injury. Even in the second edition, which focuses on activities below the threshold of war, this remains the focus.

3.2.3 Rules Concerning Neutrality

Both editions of the Tallinn Manual provide the same rules on neutrality, which are listed in a dedicated chapter of the manuals at the end. Some further rules in other chapters of the manuals are concerned with neutrality. Since the second edition of the Tallinn Manual claims that it “superseeds” the previous edition and since the rules relevant for neutrality have remained unchanged, this thesis does not compare the two manuals and provides all references listed (e.g., rule numbers) to the second edition of the manual.

The rules treating neutrality are rules 127 and 129 (both in Chapter 17 on the *Conduct of Hostilities*), and rules 150–154 (all in Chapter 20, which is devoted to neutrality). The rules are accompanied by commentaries. The rules are listed in the following and discussed taking the commentary into account.

- **Rule 127:** *In cyber operations, it is prohibited to make use of flags, military emblems, insignia, or uniforms of neutral or other States not parties to the conflict.*

This rule protects a neutral country from abuse of its symbols. It does not significantly contribute to a deeper understanding of neutrality in cyberspace and so further discussion is omitted.

- **Rule 129:** *The use of cyber operations to enforce a naval or aerial blockade must not have the effect of barring, or otherwise seriously affecting, access to neutral territory.*

This rule focuses on the effect of a cyberoperation on matters of conventional warfare. It protects a neutral country’s interest with respect to territorial blockades. A more interesting although not directly connected question for the topic

of this thesis would be what would happen in case of a “cyberspace blockade”—although it is questionable whether such a blockade would even be possible: A cyber blockade would detach a country from any access to cyberspace. However, such a scenario is highly unlikely: A country could always use satellite communication in order to omit any disconnection of its cable based Internet connection. Further workarounds for a blockade are plausible, for example the construction of a line-of-sight based radio connection into a country that is not affected by this blockade. A scenario of a cyber blockade has never so far occurred and would also be questionable practice with respect to international humanitarian law, as it would include obstructing civilians’ access to potentially crucial information systems required for survival in a conflict. The rule is therefore not discussed any further.

- **Rule 150:** *The exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited.*

The commentary explains that this rule addresses operations that are specifically aimed to “detrimentally affect” a neutral country’s infrastructure and that the inviolability of a neutral country’s territory, as defined in The Hague Conventions, is considered to be part of international customary law. It also states that operations, which only “pass through” such infrastructure (i.e., routed traffic) do not fall under this rule, which would be in-line with the interpretation of The Hague Convention in Section 3.4. However, the commentary to the rule also defines two exceptions, which significantly weaken the protective character of the rule:

First, side-effects of attacks between the belligerents may negatively affect neutral infrastructure. This is deemed the case when such side effects are not foreseeable—which is in-line with conventional neutrality law, where states are expected to take precautions where it may plausibly be assumed that a neutral country’s territory could be affected. However, side-effects are also defined to be legitimate, in case the interest of the attacker outweighs the interest of the neutral. As this principle is not limited to operations that fit the Tallinn Manual’s definition of an attack²⁰ but cyberoperations in general, it seems to significantly undermine the principle of inviolability of neutral territory as outlined in conventional neutrality law: a cyberoperation affecting a neutral country’s critical

²⁰What is considered a cyberattack under the Tallinn Manual is outlined in Rule 92 and its commentary.

infrastructure, or even the functioning of information systems in a neutral country, would be legitimate according to the rule's commentary—in clear violation of conventional neutrality concepts and, in fact, contradicting to the rule itself. The application of the commentary to the rule, as written in the Tallinn Manual, would therefore weaken the very strict inviolability defined in conventional neutrality law. No plausible reasons for such a breach of conventional neutrality law are outlined in the commentary. It should therefore be assumed that the rule was authored by representatives from countries carrying out offensive cyberoperations, who have a clear interest in weakening the protection offered under neutrality law in order to increase their scope of action. This thesis considers the reasoning in the rule's commentary to not be in-line with conventional neutrality law and, therefore, discards it as not plausibly applying for neutral countries in cyberspace. The rule itself (without the commentary), on the other hand, is considered to be in-line with conventional neutrality law.

Second, the commentary formulates that neutral cyberinfrastructure “*may lose its protection*” in the case outlined under Rule 153 and, in case the neutral infrastructure is not located within the neutral country's territory, it does not fall under the law of the protection of a neutral's territory.

Even though the rule, if read without the commentary, seems to be in-line with conventional neutrality law, the commentary weakens the rule such that it may become impractical to claim protection under neutrality since it is difficult to prove that side effects might have been foreseeable. Also, it is difficult to determine whether the interests of a belligerent are considered higher than the interests of a neutral and, therefore, a belligerent might exploit this ambiguity. The rule seems to have been written with particular attention given to the interests of major powers, who conduct offensive cyberoperations on a regular basis and want to limit their responsibility for side effects of such operations on neutral countries.

- **Rule 151: *The exercise of belligerent rights by cyber means in neutral territory is prohibited.***

The commentary to this rule specifies that it covers the example outlined in Section 3.1: Both taking control remotely (through cyberspace) of infrastructure in a neutral territory as well as physical access for belligerent means is prohibited. However, the rule is weakened by the condition of attributing attacks—in particular, when private groups, individuals, companies, etc. are involved in

the attack. Commentary 3 of the rule further provides a principle contradicting the general agreement that routing traffic, even through neutral territory, is not to be considered a breach of neutrality: A very specific case of routing traffic via a neutral's government ships or aircrafts (i.e., neutral infrastructure located outside neutral territory) is outlined, which would be considered a breach of neutrality law. On the other hand, the general principle of not considering routing through public networks in neutral territory a breach of neutrality is upheld by referencing the respective articles of The Hague Conventions outlined in Section 3.1. Yet, the case of routing traffic via a neutral's government ships or aircrafts is already covered by the notion of a *public* network: Either the network on a neutral country's vessel etc. would be restricted (e.g., for government purposes), in which case passage of messages is already prohibited *per se*, or it would provide infrastructure open for public routing of Internet packets, in which case it should not be considered a breach of neutrality law: The network *per se* is a public communication infrastructure not purely for military purposes, since public traffic is routed through it—therefore, also belligerent traffic can be routed through it without the network provider—in this case a country—taking any responsibility for the traffic routed automatically through the publicly accessible routing infrastructure.

It is further mentioned that a minority of experts held the opinion that routing in general, even through public networks in neutral territory, is considered a breach of neutrality law. While this might seem sound from a non-technical perspective, it is not practicable concerning the technical givens of how routing algorithms work (see Chapter 2) and also neglects the general idea of the respective articles on “message passing” in The Hague Conventions, as already outlined.

Thereafter, the commentary discusses whether “cyber weapons”²¹ may be transported through a neutral country's territory, be it virtually (through routing in cyberspace) or physically. The commentary believes that cyber weapons may not be transported through neutral territory in either case. However, these reflections neglect Article 7 of Document V of The Hague Conventions, where the export or transport of arms and ammunition is allowed. The argument applied in the commentary refers to Article 2 of Document V, which forbids belligerents to move troops or convoys through neutral territory. However, having goods moved, for example, tanks on a train operated by a civilian transport provider,

²¹See discussion further below on the Tallinn Manual's approach to defining the term “cyber weapon”.

would rather fall under Article 7—similarly, routing should presumably rather be considered under Article 7, even if it is applied to a “cyber weapon”, since non-cyber weapons could also be transported through a neutral country’s territory, as long as this is not done by means of convoys or troops controlled directly by the belligerent. The only condition set in The Hague Conventions is that of Article 9, which defines that any restrictions on transport or the use of communication infrastructure, which is set by the neutral, is to be applied equally to both parties.

Generally, the rule is in-line with and confirms the findings in the previous subsection on the use of computer systems located in neutral territory. However, some of the commentaries seem to contradict conventional neutrality law. The interpretation of the law, stated by this thesis, is presumably more accurate for the reasons earlier outlined and is taken as the basis for any further considerations of this thesis.

- **Rule 152:** *A neutral State may not knowingly allow the exercise of belligerent rights by the parties to the conflict from cyber infrastructure located in its territory or under its exclusive control.*

The commentary repeats that this rule does not concern passage through public and open networks, such as the Internet, for reasons outlined under Rule 151 (although this might be considered slightly contradicting the idea of cyberweapons not being allowed to be transmitted through cyberspace). However, private or restricted networks, for example, set up by the belligerents previously to the war on neutral territory, or internal government networks of the neutral country, may not be used by the belligerents in an armed conflict and the neutral country explicitly needs to restrict and prevent any such attempts it discovers. Otherwise, the commentary agrees that the usage of any systems (e.g., computers, servers, etc.) by the belligerents for attacks located on neutral territory would breach neutrality law and their use by belligerents should be prevented by the neutral country.

An important finding of the commentary is that any preventive or restricting steps taken by the neutral country, even if including “force” in cyberspace, cannot be considered a hostile act—which has also been a finding in the previous subsection (see also “hack back” in Chapter 2). The commentary further states

that there is a general understanding of the necessity of at least basic monitoring by the neutral country of any operations on its government (or other non-public) networks that could constitute a breach of neutrality.

- **Rule 153:** *If a neutral State fails to terminate the exercise of belligerent rights on its territory, the aggrieved party to the conflict may take such steps, including by cyber operations, as are necessary to counter that conduct.*

This rule answers the question *what happens if a neutral country fails to comply with its obligations?* The commentary states that intervention in case of non-compliance with (relative) neutrality obligations is generally accepted but principles of proportionality apply:

1. The rule only applies, when there is a negative effect on a belligerent;
2. the violation of neutrality by one of the belligerents needs to have yielded a serious military advantage, in order for the other party to be allowed to interfere on neutral territory—minor incidents do not suffice;
3. there must be no feasible and timely alternative; i.e., the rule “*only applies if the neutral State is either unwilling or unable to comply with its obligations under Rule 152*”;
4. the neutral state needs to be notified in advance and given sufficient time to respond and the aggrieved may only apply as much force as necessary.

In the scenario presented in the previous subsection, this rule would be applicable when the neutral country fails to terminate a belligerent activity conducted through a computer system located on the neutral’s territory.

While no specific rule of The Hague Conventions is referenced (and also the author of this thesis sees no article that would directly support this rule), it is generally considered to be within customary international law, also by the author of this thesis: It is reasonable to allow intervention, in case a neutral would abuse its neutrality or would not be able to respond adequately and its infrastructure is abused by one of the belligerents for seriously detrimental action against its opponent; the rule prevents neutrality becoming a potential liability for belligerents and the international system in general. It ensures there is sufficient interest in maintaining neutrality as a concept, also by belligerents. Even though it might seem counter-intuitive, this rule supports the credibility

of the concept of neutrality, since it avoids that it can be used as a mere label without following the required obligations. On the other hand, the rule also implicitly expects the neutral to possess a minimal capacity for conducting CNOs, which can counter potential attacks; it implies that neutrality has to be *armed* (see also the definitions of permanent neutrality later in this thesis).

- **Rule 154:** *A State may not rely upon the law of neutrality to justify conduct, including cyber operations, that would be incompatible with preventive or enforcement measures decided upon by the Security Council under Chapter VII of the Charter of the United Nations.*

As outlined in the commentary, this rule underlines the prerogative of UN Security Council decisions, as defined for UN member states in the UN charter. In particular, a Security Council decision could justify the application of force (through “cyber means”) also by the neutral state, without that state losing its neutral status with respect to a conflict. However, the rule is not based in conventional neutrality law and should rather be seen as an additional clarification of the Security Council prerogative with respect to UN members. Furthermore, the example in the commentary concerning the application of force through “cyber means” by a neutral state seems to be in contradiction to general practice: A Security Council decision as would be applicable to this case would usually either justify the application of force by a specific state (or group of states) by means of a mandate (which usually follows an explicit expression of willingness of those states) or defines sanctions that can be implemented through national law (e.g., in order to restrict financial transactions or access to financial assets). However, a dictate of direct hostile action—also by the neutral state—against a state is unprecedented. It is unlikely and would not only breach general principles of neutrality (see upcoming sections) but also general principles of countries that restrict their armed forces to actions for purely defensive purposes. The example raised in the commentary seems unrealistic and not in line with the general idea and principles of neutrality, while the general applicability of the respective rule for any UN member does not seem to be a matter of contention. This thesis agrees with the rule in that the UN Security Council may mandate members willing to deploy their armed forces (also in cyberspace) and that, under a UN Security Council decision, certain belligerent activities could be considered not to be a breach of neutrality. For example, as outlined in The Hague Conventions, if the UN Security Council would mandate the neutral to

take action in order to restore its neutrality. However, a forcing of a neutral to undertake belligerent actions that go beyond activities required to uphold or defend a neutral status would presumably not be according to neutrality law as codified in The Hague Conventions. The rule is not further discussed here but it is noted that it might provide an interesting case for the limits of neutrality practice by states.

The chapter on neutrality in the Tallinn Manual further contains some general remarks: It is stated that the neutrality-related rules are derived from customary international law, which The Hague Conventions form part of. This would imply that the rules as stated are assumed to be of binding character by the experts (see discussion on whether the rules are binding in the previous paragraph). The author of this thesis slightly disagrees with this reasoning for reasons already outlined.

Furthermore, the term “neutral” is explained as applying to a country that is not part of a conflict between third parties. Hence, it resembles the finding of the previous subsection that neutrality law only defines neutrality *relative* to a specific conflict. In this context, three main goals (or principles) of neutrality are defined.

They are to: “

1. *protect [relative] neutral States and their citizens against the conflict’s harmful effects;*
2. *safeguard [relative] neutral rights, such as engaging in commerce on the high seas;*
3. *and protect parties to the conflict against action or inaction on the part of [relative] neutral States that benefits their enemy.*

”

It should be noted that the points above particularly apply to *permanently* neutral states. The Tallinn Manual states that since the rules apply to third parties in general, they are particularly applicable “*in modern armed conflict*”. This may be understood as an indication towards a general applicability for any country that is not part of a conflict between two other parties—without the need to explicitly declaring neutrality in the first place.

The commentaries further address the difficulty of routing of malevolent traffic and consider this a difficult reality and emphasise that routing traffic through a neutral country cannot be considered a violation of neutrality, as has already been stated in

some of the rule-specific commentaries. Moreover, it is stated that any infrastructure on a neutral state's territory is considered neutral in the sense that it is subject to the state's jurisdiction and also protected by the neutral state's sovereignty.

3.2.4 Discussion and Conclusions on the Tallinn Manual

The rules and commentaries presented above do not generally contradict the findings of Section 3.1. However, there are also some noteworthy differences in the Tallinn Manual when compared with the analysis of conventional neutrality law and its application to cyberspace in Section 3.1. These are shortly summarised in the following:

First, it should be noted that the general commentary in the chapter on neutrality seems in line with the findings of this thesis. It also states some fundamental principles of neutrality, which do not contradict the analysis of international law in this thesis.

Second, some rule-specific commentaries do not appear to align with the findings of the previous subsection and, in some cases, also seem to contradict conventional neutrality law. In particular, this was the case when speaking about routing in general and routing of "cyber weapons" through neutral territory. The noteworthy differences to the findings of this thesis are shortly discussed in the following:

- The commentary to Rule 150 seems to significantly weaken the rights of a neutral power: Side-effects of attacks are allowed on neutral territory if unforeseen by a belligerent or in case the interests of a belligerent power to conduct an attack are higher than the interests of the neutral power to protection of its networks. The commentary neglects the strict protection of neutral territory of conventional neutrality law and the author of this thesis notes that it particularly favours the interests of a (large) belligerent power while significantly clipping the interests and rights of a neutral power. This thesis considers that the generally protected nature of systems located on neutral territory is given through conventional neutrality law and differs with the Tallinn Manual on this point;
- the commentary to Rule 151 explains that routing of (potentially belligerent) traffic through public networks in neutral territory is not considered a breach of neutrality. On the other hand, non-public networks may not be used in case they are located on neutral territory. It is noteworthy that while this thesis agrees with the general idea of this rule, some very specific cases are outlined in the commentary that seem superfluous and may be a sign of limited technological understanding by some of the experts;

- the commentary to Rule 151 seems to directly contradict conventional neutrality law with respect to the passing of “cyber weapons” through neutral territory. This thesis bears a different view due to the respective articles of The Hague Convention and also due to technological feasibility (see Chapter 2);
- Rule 152 explains that a neutral country may use force to protect its neutrality and this thesis agrees with this approach due to a clear reference to conventional neutrality law;
- Rule 153 implies that a state requires minimal cybersecurity capabilities, including monitoring of activities on its governmental networks, in order to protect its neutrality and potentially take action against a breach of neutrality. Even though the rule does not directly reference any definitions in conventional neutrality law, this thesis agrees with it and considers the principles and ideas outlined in the commentary to be essential in order for neutrality to be an effective concept rather than an empty label that could be abused by countries that support one side of an armed conflict;
- Rule 154 applies to UN member states specifically and, as outlined, provides a very extreme example of what a neutral state would need to do in case of a respective UN Security Council decision. However, the scenario stated in the rule’s commentary does not seem plausible and applicable: The requirement to belligerent activity (i.e., outside the neutral party’s territory) would fundamentally breach multiple principles: Apart from a neutral’s pledge to general non-intervention, it would also question the principle of force being allowed for purely (and very strictly interpreted) *self-defence*. A detailed analysis of this principle is omitted here since this would be beyond the scope of this thesis. For the purpose of this thesis, however, it is noteworthy that the commentary of the rule implies an important foundation for neutrality: In order for neutrality to be successful, it requires the ideological support of major powers. In the contemporary international structures of the United Nations, these are the permanent members of the UN Security Council. A neutral country would also need to act in line with the expectations towards a neutral party of (at least a clear majority of) major powers.

Third, the general rules discussed, which outline the Tallinn Manual’s understanding of “cyber attack”, “cyber weapon”, and its approach towards espionage, reveal a strong focus on the physical impact of operations.

Furthermore, the Tallinn Manual defines the criterion of attribution for any retaliations to cyberattacks and also explains only state actors are to be considered. Even though the second edition of the Tallinn Manual is said to reflect cyberoperations in general, including below the threshold of war, the rules with regard to neutrality seem very focused on conventional warfare (i.e., they do not seem to have taken into consideration the basis for the second edition of the Tallinn Manual) and have not been updated since the first edition of the manual. The gap this reveals with respect to how neutrality should be understood with respect to cyberspace in times of peace (or *unpeace*) is, therefore, identified as a core gap of theory. In particular, cyberespionage cases that form a borderline case are reflected later on in a case study on the *RUAG Hack* in Chapter 5. The rules in international law form only the baseline for neutrality and outline the specifics during times of war; implications and general principles for permanently neutral countries with respect to cyberspace need yet to be formulated, for example by this thesis.

Finally, considering all of the above, it is noted that, in general, the findings in the Tallinn Manual seem plausible when reflected on the background of technological givens and fundamental principles and rules stated in conventional neutrality law. However, there are some significant exceptions that have been explained. The differences provide some implications for neutral countries when considering the development of the Tallinn Manuals: When consulting the list of experts from both manuals²², it is striking that there was only one representative from Switzerland for the first edition, who was from an academic background (and, therefore, had no connection to the government), and no representative for the second edition. In contrast, numerous experts from defence / military universities in the USA were present for the drafting process of both manuals. Therefore, the perspective of a neutral country and academics who have a cultural background from a neutral country might have been underrepresented—this might explain some of the slightly strange arguments found in the comments of the rules discussed, when juxtaposing them with the givens of Internet technology and conventional neutrality law.

Taking this into account and following the previous analyses of the rules and commentaries covering neutrality, the following finding appears appropriate: Where the Tallinn Manual references international law the rules seem to be in line with previous findings on international law in this thesis (with the exception of a reference to the wrong article in the case of “cyber weapon” transport through neutral territory, as presented before). However, where the rules and commentaries are rather shaped

²²See the respective sections in the Tallinn Manuals [27, 28].

by the experts' opinions, the origin of some experts from powers regularly conducting cyberoperations (such as the USA) seems to provide for a tendency to narrow the rights and protection of neutral powers.

The most noteworthy example is the legitimisation of side-effects of cyberoperations on infrastructure in neutral territory, as previously discussed. This last finding emphasises that a neutral country always must have a significant self-interest in shaping international norms, in order to protect its neutrality rights: neutrality should not be seen as an excuse for isolation but, rather, requires a vivid collaboration in international consultations and norm-shaping processes (this principle is more formally expressed as a consequence of the case study on permanent neutrality in Chapter 4). The collaboration is limited in that it cannot include a formal membership in alliances or politically binding structures (such as NATO or the EU), which would breach a strict idea of neutrality and assign the neutral country to a specific block of nations. However, a non-binding collaboration with respect to shaping norms or international rules, in particular with respect to neutrality, is in the vital self-interest of a neutral country and sufficient care should be given to participating in such processes. It seems the participation in the Tallinn Manual drafting process by Switzerland was rather limited, and, therefore, some of the rules and commentaries contradict the spirit of conventional neutrality theory.

3.3 Further Work Discussing International Law

The previous two subsections focused on The Hague Conventions of 1907, which explicitly codify the principle of neutrality in international law, and the Tallinn Manuals, which provide an interpretation of neutrality with respect to cyberspace and are limited to cases of declared war. The focus of this subsection is to present and discuss further publications that are relevant for a legal and international norms approach to neutrality in cyberspace.

The discussion of works preceding the publication of the (first) Tallinn Manual in 2013 is contained in Subsection 3.3.1:

1. A paper published in 2009 by Kastenbergh [65] outlines the general problem of cyberspace with respect to international law and touches on the question of neutrality. However, it uses a very broad understanding of neutrality, which denotes any party that does not take part in a conflict between third parties; the question is applied in a US context with respect to third-party (i.e., non-US) conflicts;

2. a paper published in 2012 by von Heinegg [66] addresses the question of neutrality in cyberspace more systematically and holistically, in a similar way as later in the Tallinn Manual and in Section 3.2 of this thesis. It was published at *CyCon*, the NATO CCDCOE’s annual conference on cyberconflict—which might explain its similarity to the Tallinn Manual’s approach;
3. Von Heinegg published a further paper in 2013 titled *Territorial Sovereignty and Neutrality in Cyberspace* [67], which was released in a law journal.

The works that were released after the publication date of the first Tallinn Manual are then split into two further subsections:

A monograph published in 2014 by Alex Spring [12], which contains an edited version of his PhD thesis on *The International Law Concept of Neutrality in the 21st Century*, is discussed in Subsection 3.3.2. It provides valuable insights due to its thorough analysis of the international law implications for Switzerland. However, its main focus does not lie in cyberspace.

Thereafter, Subsection 3.3.3, discusses further work published after the release of the first edition of the Tallinn Manual:

1. An article released in 2021 in *International Law Studies* [4] reflects on the difficulty of the application of the international law of neutrality in cyberspace. It juxtaposes the theoretical discussion with practical scenarios;
2. a report released in 2021, reflecting on the *The Law of Neutrality in Cyberspace* [40], has been released by the *Centre for Security Studies* of ETH in Zurich (Switzerland). It includes different aspects of neutrality (also from a Swiss perspective) and the problems that arise in cyberspace. Apart from expanding on the legal foundation of neutrality, it also provides a very brief historic and taxonomic overview, which seems to be based on work by the author of this thesis listed in Appendix A.

Finally, a résumé of the main findings is provided in Subsection 3.3.4.

3.3.1 Publications preceding the Tallinn Manual

Kastenberg’s article *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law* [65], which dates back to 2009, is written from a US-centred perspective, focusing on the advantage of a neutral status of states in a war. It mentions “enforcing” neutrality of states in the conventional

physical space, in case of a breach of neutrality—reading the article it almost seems that neutrality is a tool for a very strong belligerent to ensure that smaller countries do not interfere in a war and that neutrality is automatically assumed for any countries not directly involved in any hostilities. In this sense, the article might rely on a plausible divide between practice and policy: On the one hand, what is enshrined in neutrality law and policy—in the sense of a formal definition, on the other hand the reality of major power’s practice with respect to neutral states—in the sense of an instrumental definition. This would underline the requirement of neutral parties being armed with a significant capability of defending their interests, as is later discussed in Chapter 4 with respect to the term *armed* neutrality. The article further reflects on the question of whether routing through a country might violate its neutrality and speaks of the USA as a neutral country during the Georgia War in 2008 and its related cybersecurity incidents, juxtaposing this to the fact of “roughly eighty per cent of the Internet traffic” passing through publicly accessible networks located in the USA²³. While the article poses similar questions to the ones already posed in previous subsections, it does not provide any particular additional insights; its considerations focus on the first notable international cybersecurity incidents, such as those in Estonia in 2007 and in Georgia in 2008. The main findings confirm what has already been discussed with respect to neutrality law in general and also in the Tallinn Manual: The problem of routing is addressed in a similar fashion; the problem of private infrastructures being used for attacks is raised. As such the article does not provide any particular further insights.

Von Heinegg’s paper published at CyCon²⁴ in 2012 [66] addresses similar questions but from a less US-centred perspective and in a very similar manner to the Tallinn Manual. Von Heinegg formulates the claim that neutrality law does not only serve the protection of the territorial sovereignty of the neutral but also the protection of the interests of the belligerents—a claim which is found in a very similar form in one of the commentaries of the Tallinn Manual on neutrality, which has been discussed in the previous subsection: it supported the weakening of the inviolability of a neutral country’s territory with respect to cyberspace, in case this would be justified by a sufficiently high interest of a belligerent in conducting a specific operation. Since the contents of the paper are otherwise congruent with the commentaries of the Tallinn Manual (even though more in-depth), they are not discussed any further. It

²³See the introductory paragraphs of Kastenbergs’s article [65].

²⁴In full, CyCon is named: *The International Conference on Cyber Conflict*. It is hosted by the NATO CCDCOE in Tallinn. See the following website for further details: <https://ccdcoe.org/cycon/>

is noteworthy that the author of this paper was also on the editorial board of the first edition and worked as a legal expert on the second edition of the Tallinn Manual.

Von Heinegg's further paper released in 2013 [67] reflects on aspects of territorial sovereignty and cyberspace. It considers the problem of territoriality in cyberspace *per se*: As a space it is ubiquitous and anonymous—however, von Heinegg admits that in terms of the physical location of a specific piece of infrastructure, for example a server or another system, territorial sovereignty is given and, therefore, cyberspace is not beyond territorial sovereignty—at least not completely. He further emphasises that territorial sovereignty is not affected by mere espionage activities in cyberspace, even if they affect systems within the territory of a neutral country: only physical effects should be considered. In fact, he emphasises that many scholars only consider severe material damage to be an infringement of territorial sovereignty through a cyberoperation. On the other hand, von Heinegg also mentions different views, which are more strict with respect to breaches of sovereignty rights and that would consider espionage to be forbidden. These different aspects are essential when defining neutrality in cyberspace, since they determine what a neutral country may and may not do and what activities in cyberspace it might be subject to. The text emphasises that any computer infrastructure would be protected by these considerations, be it governmental, corporate, or private, as long as it is located within a state's territory. It concludes that *“the characteristics of cyberspace do not pose an obstacle to the exercise of territorial sovereignty and jurisdiction; they merely increase the difficulty of so doing.”*²⁵ This statement fundamentally supports the notion that, therefore, neutrality is a concept that is also applicable in cyberspace and with respect to cyberoperations. As such, it substantially strengthens the case of conducting this thesis.

The text further outlines some basic duties of nations with respect to sovereignty and neutrality: an International Court of Justice decision is cited, which claims that states are obliged *“not to allow knowingly its territory to be used for acts contrary to the rights of other States”*.²⁶ This finding is also relevant with respect to the duty of neutral countries to prevent such activity from infrastructures on their territory. With respect to cyberspace von Heinegg provides further contents very similar to those of his previously discussed publication at CyCon and it is therefore not discussed here any further. The insights with respect to sovereignty and espionage are very useful for understanding the possible practice of neutrality in cyberspace, which is taken forward in Chapter 5.

²⁵See page 134 in Von Heinegg's paper [67].

²⁶See page 135 of Von Heinegg's paper [67].

3.3.2 Monograph by Alexander Spring

The monograph by Alexander Spring from 2014 [12], which contains a published version of his PhD thesis, provides a detailed approach to the Swiss understanding of neutrality. This is provided from a legal perspective and based on international law while not being limited to this perspective. Spring also supports this thesis' approach of focusing on Switzerland as the "*neutral state par excellence*"²⁷. He provides a number of useful insights for the understanding of what neutrality is from a legal perspective and beyond, which are discussed in the following, in order to contribute to a foundation for understanding neutrality.

First, Spring elaborates on the origins of neutrality. He explains that "*at first, neutrality was a political term before it evolved into a legal term*".²⁸ This supports the statement made earlier, that there is more to neutrality than the legal perspective: there is also the political perspective of neutrality policy and how it may be implemented. Spring defines the terms of *relative* and *permanent* neutrality. Relative neutrality, therefore, denotes the concept of neutrality towards a conflict between third parties. It is always a "*reflex of war*"²⁹. This also counts for permanent neutrality, since it is also defined with respect to war—only that it describes a state's policy to prevent taking sides even before a conflict between other states arises. Relative neutrality always has to be explicitly declared relative to a specific war between third parties and generally refers to the concept of neutrality codified in international law. Spring notes that relative neutrality *must* be declared—it may not be automatically assumed that non-belligerent powers are neutral and fall under the obligations and protection provided by the law of neutrality. Spring briefly provides further elaborations on different types of neutrality, which are covered in Chapter 4, where this thesis defines a neutrality taxonomy.

Second, Spring provides a brief history of the practice of neutrality, from a Swiss perspective. Some of the contents are discussed later in Chapter 4, along with further sources. He summarises the understanding of neutrality in the 20th century as follows:

*"Neutrality is the status of a state, which does not participate in an armed conflict between other states."*³⁰

²⁷See page 2 of [12].

²⁸See page 7 of Spring's monograph [12].

²⁹See page 34 of Spring's monograph [12].

³⁰See page 34 in Spring's monograph [12].

Third, Spring provides a very brief reflection on neutrality in cyberspace³¹. It is specifically with respect to “cyber warfare”. Spring agrees with the overall tendency of publications which consider neutrality law and international law, in general, to be applicable in cyberspace. His focus on what he calls “cyber neutrality” is through the lens of relative neutrality. He provides a classification of Computer Network Operations (CNO) into Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defence (CND), as has been presented in Chapter 2; only CNA is relevant for relative neutrality law. Spring agrees with the major points made in this section with respect to how relative neutrality is applied in cyberspace; i.e., routing of any traffic should not be considered a breach of neutrality, while launching an attack from systems located on a neutral country’s territory would.

Furthermore, he takes a similar view as the author of this thesis with respect to the protection of neutral territory from side-effects of CNA directed at a third party:³²

“The use of neutral computer system [sic!] as botnets as well as a spilling effect of the CNA into the cyber infrastructure of the neutral would count as a violation of the right of relative neutrality. The same applies of course to the damage of foreign infrastructure though [sic!] CNAs which has an indirect negative effect (collateral effects of hostilities) to the infrastructure of the neutral state or its territory, (e.g. disruption of electricity or nuclear fallout).”

Spring is very clear in this case with respect to the right to protection of a neutral’s infrastructure and territory from harm through any belligerents. He does later cite the Tallinn Manual in that it says that if side-effects were unforeseeable they do not violate neutrality protection rights—however, he does not mention that he agrees with this and his earlier statement seems to indicate a contradictory view, which would be in-line with the findings of this thesis earlier in this chapter. Other than this, Spring’s text does not add anything substantial to the understanding of relative neutrality in cyberspace not already outlined in this section and it does also not elaborate on the implementation of permanent (or other) neutrality in cyberspace.

In conclusion, Spring’s monograph provides a number of meaningful insights relevant to this thesis, in particular with respect to the classification of different types of neutrality (i.e., relative versus permanent). Some contents are outlined and relied on later in this thesis, in order to define neutrality and derive conclusions for cyberspace.

³¹See Section 3 of Part IV in Spring’s monograph [12].

³²See page 249 of Spring’s monograph [12].

3.3.3 Further Publications released after the Tallinn Manual

Two publications dating from 2021 are also concerned with neutrality from an international law perspective. They are discussed in the upcoming two paragraphs.

Neutrality Law as Understood by Neuman

The article published by Noam Neuman in 2021 in *International Law Studies* [4] elaborates on the “reality” states are confronted with, when considering neutrality law in cyberspace. Its approach towards neutrality is very similar to the approach of the Tallinn Manual and further publications already discussed. The text provides three realistic scenarios concerning relative neutrality in cyberspace: The first scenario elaborates on the difficulty with respect to applying the law of neutrality to the routing of belligerent traffic through a neutral country—this example is not covered any further, as it has already been exhaustively discussed previously and in other publications. The second scenario focuses on collaboration between countries with respect to espionage and technical cyberdefence/cybersecurity incident mitigation capabilities. This is usually done between national *Computer Emergency Response Teams* (CERTs, see Chapter 2) of different countries in what is known as a *CERT Network*. The scenario outlines a case where a neutral country might participate in such a *CERT Network* with other countries, including a belligerent power, say *State A*: Information obtained by the neutral state would be passed on to the CERT Network, including State A. In case information about an imminent attack by State A’s opponent, State B, would be passed on, this could enable State A to defend itself or “thwart” a cyberattack.³³ Neuman outlines this might be a breach of neutrality according to Article 6 of Document XIII of The Hague Conventions of 1907 [55], since the article prohibits the neutral to supply “*war material of any kind whatever*”³⁴. There are a number of questionable points in Neuman’s argument in this scenario:

1. It is questionable whether sharing of information would classify as “material” under Article 6 of Document XIII. It may be assumed that the term material, as used here, rather refers to “*a physical substance; a material thing*”³⁵, since it is used as a compound (“war material”) in connection with kinetic war and is part of a listing of other terms relating to physical war-related items, such as “*war ships*” or “*ammunition*”.

³³See Page 791 of Neuman’s article [4].

³⁴Cited by Neuman’s article [4], from Article 6 of Document XIII of The Hague Conventions of 1907 [55].

³⁵See the online edition of the Oxford English Dictionary [16], when searching for the term “material”, under section B.1.a, as accessed in 2023.

2. Sharing of intelligence is not restricted to cyberspace. Similar scenarios are possible with respect to traditional, kinetic warfare, where information about an imminent (kinetic) attack could be shared by a neutral country with one of the belligerents. Nevertheless, the sharing of information with respect to cyberspace might be more delicate than with respect to traditional kinetic warfare.³⁶
3. It is unclear to which extent sharing is done within the CERT networks: What type of information is shared? In case certain vulnerabilities are disclosed within the CERT Network this might be very different to a case where it is clear that a cyberattack against a belligerent who is part of the network is imminent. In the latter case, a breach of neutrality is more likely (even though not clear) than in the former—however, this is not due to a provision in international law and may rather be an interesting scenario for customary law and norms with respect to permanent neutrality.

The second scenario, while interesting for neutrality in general, does presumably not fall under the law of neutrality, since it does not involve physical objects. However, it provides an interesting scenario for considerations on permanent neutrality.

The third scenario outlined by Neuman considers a privately owned “*Web Application Firewall*” (WAF)³⁷, which protects the military website of a belligerent State A. The website is used by State A to recruit reserve-duty soldiers. The servers for the WAF service are located in a neutral country. The question posed by the scenario is: What happens in case State B (the opponent of State A), aims to shut down the websites of State A? Neuman argues that there is a dilemma in interpretation, which yields an ambiguity depending on which articles from The Hague Conventions are used for interpreting the situation. However, his analogy creating the dilemma does not seem to work when considering it from a technological perspective: A WAF service would usually route all the traffic through its servers; even if provided by a private company it would be part of the website system of a military power. Any

³⁶Furthermore, during the Russian invasion of Ukraine in 2022, it seems there was a substantive collaboration between British intelligence services and Ukraine. Therefore, Britain would need to be considered a belligerent in this conflict—however, this does not generally appear to be the case.

³⁷A WAF is a common concept provided as a service by providers. However, it is evident that it effectively routes any traffic through the servers of the service provider (or the service provider needs to deploy the service to the servers of the customer). In any case, the WAF would be considered to be part of a webserver infrastructure and, therefore, should not be located in the territory of a neutral country in case it protects government or military infrastructure of a belligerent. Many explanations on WAF services are available, some websites explaining what has been outlined in the previous sentences may be found online, such as an article published on Cloudflare (accessed 2022) [68] or written by Sundar (2019) [69].

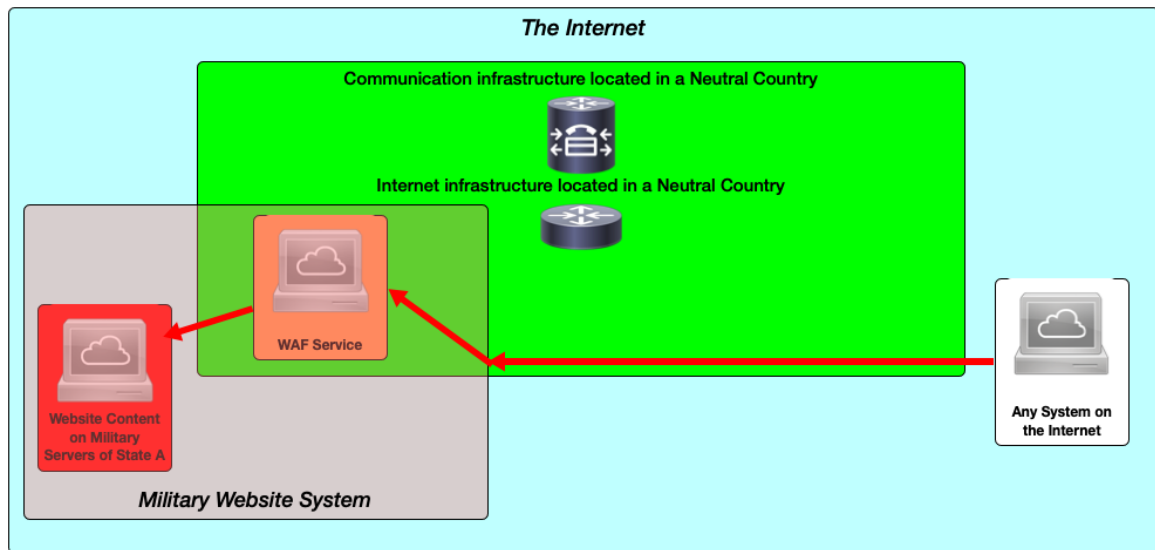


Figure 3.2: Illustration of Neuman's [4] WAF scenario.

traffic routed to the recruiting website would reach the WAF servers first—therefore, the WAF service bought from the private company is purely for military purpose and provides a direct connection to the military servers. An illustration provided in Figure 3.2 attempts to better explain the situation: Any system on the Internet will need to connect with the WAF service located in the neutral country, in order to access the military recruiting website of State A. It would, therefore, need to be considered part of the military website infrastructure of State A, and locating it on systems within a neutral country would, for reasons outlined in Section 3.1 and Section 3.2, constitute a breach of neutrality.

Overall, Neuman argues that the ambiguity with respect to interpretation of scenarios of relative neutrality in cyberspace is high, and that cyberspace and the neutrality law, based in The Hague Conventions, are not compatible. However, as has been shown previously, this is not the case. Nevertheless, dilemmas might arise from a missing consideration of technological and existing legal considerations. The article assumes that neutrality automatically arises for third-party countries in case of an armed conflict. As shown earlier though, this is not generally considered to be the case: neutrality has to be declared with respect to a conflict. Nevertheless, Neuman makes an important point with respect to the application of neutrality law in cyberspace: The interest by many states seems to be low (as also the unchanged content on neutrality in the second edition of the Tallinn Manual shows), and he also outlines that the emphasis of the second edition of the Tallinn Manual on conflicts below the threshold of war poses major problems for the general concept of neutrality.

While the problems raised might not be applicable for neutrality law per se, they do seem of relevance for the applicability of problems for permanent neutrality, which is discussed later on.

Neutrality Law as Summarised by Cordey et al.

A report released at the end of 2021 by Cordey et al. at ETH [40] provides an overview of discussions in neutrality law and a taxonomy of terms related to neutrality theory. The report relies on findings of the author of this thesis.³⁸ There are no substantial additions to what has already been discussed.

3.3.4 Key Findings on Further Legal Work

The passed subsections have analysed and discussed publications covering neutrality law, which have emerged over the past years (and more may exist). However, most of them do not substantially differ from the Tallinn Manual’s findings with respect to neutrality law. Nevertheless, the following list provides some noteworthy points:

- There is a difference in terminology between *relative* and *permanent* neutrality. The former refers to the definition in international law, while the latter is a term shaped by norms, customary law, and traditions in practice by states that define to adhere to neutrality also during times of peace (or before wars emerge). Furthermore, a general definition of the abstract concept of neutrality has been provided;
- Internet routing through public networks is generally considered unproblematic with respect to neutrality law;
- points outlining a strict inviolability of neutral territory seem more convincing with respect to the articles found in neutrality law—some discussion may be possible as to whether unforeseeable effects of cyberattacks may be tolerable or not;
- concepts of sovereignty and neutrality are applicable to cyberspace, even though the territorial aspect is different to conventional warfare;

³⁸In particular, the ETH report references a paper *On Neutrality and Cyberdefence* [43] released in 2019, which provides an overview of the historic and legal aspects of state neutrality and explains some of the challenges cyberspace poses to this. It is listed in Appendix A

- discussion is possible with respect to whether espionage operations might be in conflict with the abstract concept of neutrality. However, they are not covered by international law (also for conventional conflicts) and many publications further determine that neutrality law (since it refers to warfare) only applies in case of physical effects;
- von Heinegg defines a duty to prevent hostile action to be conducted from a neutral’s territory (this is referred to as the “prevent duty” later in this thesis);

In general, it seems like most questions may be quite clearly answered with respect to relative neutrality and a strict interpretation of warfare referring to physical damage or injury. However, when considering permanent neutrality and espionage, many questions arise that the upcoming sections will answer.

3.4 Conclusions for the Legal Perspective

The analyses and discussions of existing international law and publications have shown that neutrality is a concept which is applicable to cyberspace. This has been shown from a pragmatic perspective by means of directly interpreting the law of neutrality with respect to the characteristics of cyberspace. This view is strongly backed by the fact that the Tallinn Manual considers neutrality and its application to cyberspace. Furthermore, multiple publications address the problem of neutrality in cyberspace, indicating a general consensus of scholars to the application of neutrality in cyberspace—although with some variety on how neutrality applies in cyberspace. One publication (von Heinegg in 2013 [67]) specifically addresses state sovereignty as a prerequisite and claims that it, as well as other concepts in international law, are transferable to problems posed by the characteristics of cyberspace. Since neutrality is based on a territorial approach and, therefore, also on questions of state sovereignty, it follows that it is also applicable to cyberspace. However, von Heinegg admits that cyberspace adds a level of complexity.

On the other hand, the findings of previous subsections have also identified various gaps: what about *permanent* neutrality? What about espionage operations in cyberspace? In particular since views on whether espionage in cyberspace is permitted or not differ.

Some findings have also provided a better understanding of some fundamental principles for neutrality outside of its legal definition: A neutral state needs to be supported in being neutral by major powers. The neutral also needs to constantly

engage with the surrounding world in order to shape and advocate an understanding of cyberspace—this has been outlined by means of reflections on the Tallinn Manual process and the shortcomings of the manual with respect to a perspective from a permanently neutral state.

In contrast to common intuition, neutrality does not benefit from isolation: it requires a connection with the world beyond, even though not through alliances or ties that might yield the neutral to be dependent on one single major actor. The permanently neutral needs to maintain relations broadly, in order to promote an understanding of what neutrality is and to explain what its benefits are for the global community.

The upcoming chapters address exactly the gaps identified by the current chapter: they reflect on the history and definition of permanent neutrality and illuminate the difficulties of permanent neutrality in cyberspace, while also providing some solutions. The current chapter provides some foundations for these reflections since permanent neutrality needs to be considered as a strict subset of relative neutrality: As is evident from the discussions and analyses in this chapter, permanent neutrality is the commitment to prepare for relative neutrality even before an armed conflict arises.

Chapter 4

Conventional State Neutrality: History and Theory

The previous chapter introduced neutrality from an international law perspective—known as *relative* neutrality. It further elaborated on existing approaches towards the application of neutrality law in cyberspace. As outlined in the previous chapter, permanent neutrality is not directly codified in international law at the point of writing this thesis; it relies on customary international law, i.e., norms, state practice, and historic precedent. As stated in previous chapters, the example *par excellence* for a permanently neutral country is Switzerland. It has been permanently neutral since 1815. Hence, this chapter focuses on Switzerland. It aims to derive patterns from the history, the literature, and from case studies on neutrality. The “patterns” found during this process are formalised as conclusions, lemmas, and definitions; moreover, conventional state neutrality terms are defined in the sense of a *taxonomy*. This formalised understanding of conventional neutrality is what this thesis refers to as *neutrality theory* or, more specifically, as *conventional neutrality theory*. A major output of this chapter are the various definitions of neutrality terms. In order to provide the reader with a first overview of these definitions they are listed in Table 4.4. Furthermore, an illustration is provided depicting some of these terms within the potential range of permanent neutrality, as is later discussed in this chapter. The illustration is shown in Figure 4.1 and discussed in Section 4.4.

This chapter is structured as follows: A case study based on the history of neutrality (focusing on events since 1815) and a discussion of neutrality developments including the 20th century is provided in Section 4.1. The case study mainly relies on a discussion of historians’ approach to the topic, as well as some statements from decision makers and experts released as part of a monograph on neutrality published by Kreis in 2014 [17]. Thereafter, Section 4.2 provides an overview and discussion of

Term	Definition summary
Neutrality	Philosophical / etymological term denoting impartiality, not restricted to a political / legal meaning.
State Neutrality	Neutrality in the sense of impartiality, when applied as a concept for states in the international “arena”.
Military Non-alliance	Independence of a state from an alliance system—not necessarily subject to not being on any side or restricted by any neutrality restrictions.
Relative Neutrality	State neutrality as defined in international law; strictly speaking in international law neutrality is always relative to a specific conflict.
Permanent Neutrality	Commitment of a state to remain neutral even before a conflict arises; norms-based.
Geostrategic Neutrality	Declaration of a territory / state as neutral based on its geostrategic relevance (such as for Switzerland in 1815).
Armed Neutrality	Not a type of neutrality. Denotes the necessity of a neutral possessing an effective defence capability, in order to credibly be able to uphold its neutral status.
Differential Neutrality	Permanent neutrality under the aspect of the state integrating itself into established international structures, such as the UN. Often refers to Swiss neutrality during its membership in the League of Nations (between the World Wars).
Active Neutrality	Similar to differential neutrality. Swiss neutrality as implemented since the early 21 st century. Term coined by Federal Councillor Micheline Calmy-Rey.
Integral Neutrality	Form of permanent neutrality which refrains from an integration into international structures due to their irrelevance and evolving international tensions. May be described as an isolationist approach in times of international instability.
Cooperative Neutrality	Term coined by federal Councillor Ignazio Cassis in 2022 and rejected by the Federal Council; it denotes a stronger formalisation of collaboration with western countries and alliance systems. Austria’s neutrality may be considered to be cooperative.

Table 4.1: Summary of neutrality definitions, as defined in Section 4.4.

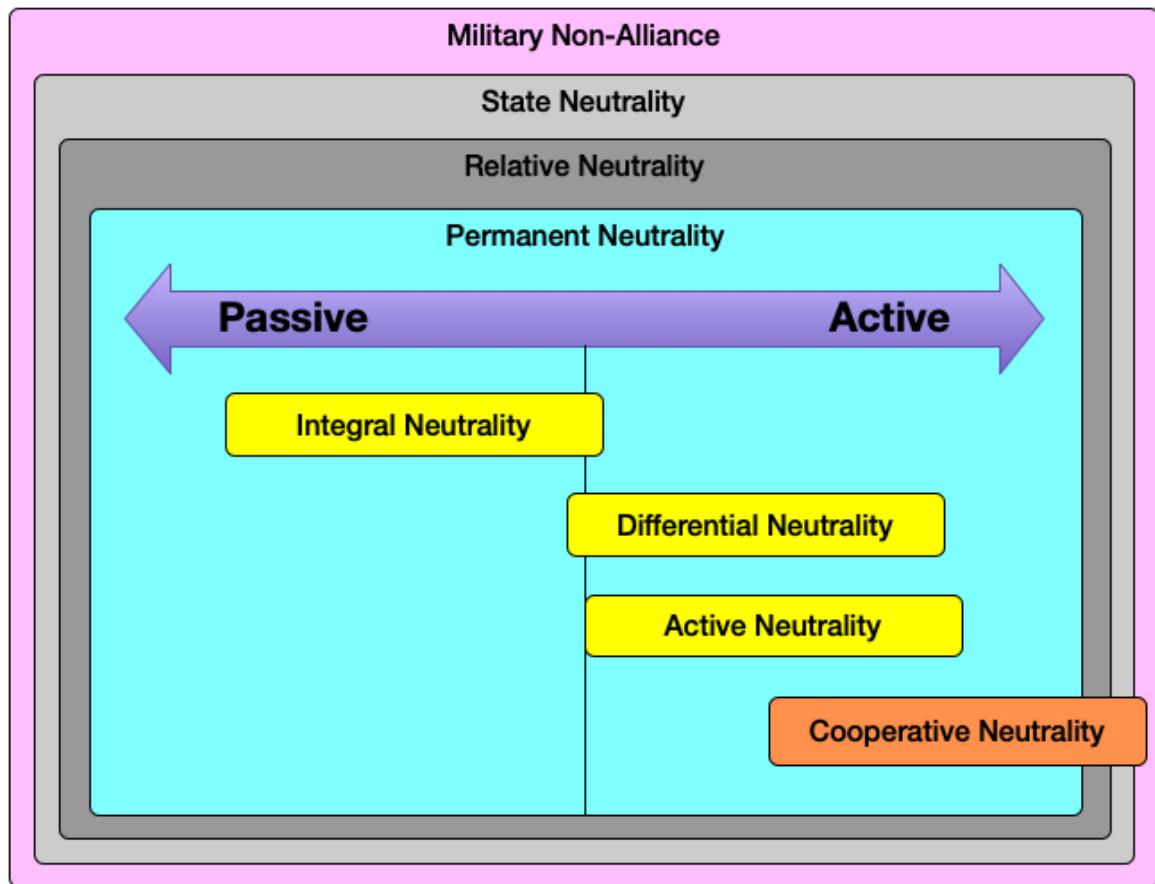


Figure 4.1: A visualised summary of the findings on state neutrality and its taxonomy, as discussed in Section 4.4.

the most recent developments of neutrality since the beginning of the 21st century, with a particular focus on the terms *active* and *cooperative* neutrality. The subsection is set up as a case study, which also incorporates discussions on the background of the Ukraine conflict, including developments in 2022. Section 4.3 synthesises the most important themes in the previous sections. On the basis of the findings, Section 4.4 defines a taxonomy of neutrality (including definitions of terms) that may be useful as a theoretical framework for reflecting on neutrality. It is a major contribution of this thesis to academia and may be referred to as *conventional neutrality theory*.

What this chapter does not cover is cyberspace—the aim of this chapter is to provide a foundation upon which considerations for cyberspace can be developed in Chapter 5.

4.1 A Historical Case Study on Modern Neutrality

The aim of this section is to discuss the concept of *permanent* neutrality through the lens of history: By analysing the history, different aspects and implementations of neutrality are discovered and analysed, which lead to the definitions in Section 4.4.

As outlined earlier, permanent neutrality also covers activities below the threshold of war. Therefore, the *role* a permanently neutral country takes in such conflicts (e.g., the role of a mediator) or the definition of what permanently neutral countries should or should not do in times of peace and war may be of interest. While analysing publications on the historic evolution of neutrality, a particular focus is laid on synthesising themes and principles that may be used to characterise, understand, and predict state neutrality in a theoretical framework.

The publications discussed are selected with a focus on their taxonomic relevance. Pure historic outlines are omitted, while texts that aim not only to explain the history but also to prescind the nature of neutrality with respect to a taxonomic definition are prioritised.¹ The publications discussed in the following mainly focus on developments from 1815 onwards—as already outlined, Switzerland implemented permanent neutrality since this date (while its foreign policy prior to the napoleonic wars may rather be referred to as a form of *military non-alliance*).

The contents of the following subsections are shortly outlined in the following:

First, a general overview of historic events with relevance for the development of permanent neutrality as a state doctrine of Switzerland are presented in Subsection 4.1.1. The aim of the section is to provide the reader with a general overview of historic events, such that the subsequent subsections can mainly focus on relevant

¹A publication authored by André Holenstein in 2014 [70] on how Swiss neutrality came to be is, for example, omitted, since it does not provide particular insights for creating a taxonomy of neutrality. It focuses on the tension between Switzerland’s interdependence with and its alienation from European politics on the foundation of the “national identity” perspective on neutrality. The majority of the monograph is a history of Switzerland with a particular focus on alienation and interdependence. Holenstein defines neutrality as a matter of national self-perception and as crucial to Swiss identity. He explains that, while some legends go back as far as 1515 in declaring the starting point of Swiss neutrality, neutrality did not develop overnight. Rather, it developed gradually over the centuries. He sees the root of Swiss neutrality in the common geopolitical interest of the major European powers in the alpine passes not being governed by any of the other major powers. Holenstein emphasises that Switzerland does not have a far-reaching diplomatic tradition—contrary to any intuition derived from its present-day function as a host country to international organisations. Due to internal conflicts and the very weak competencies of the federal diet of the Old Confederacy, Switzerland did not mandate diplomats with any meaningful power. This scepticism towards foreign relations in general was further supported by the Swiss populus after the foundation of modern Switzerland in 1848.

contents found in any publications and do not need to fully reiterate the general context of events.

Second, Subsection 4.1.2 reflects on the contents of a small collection of essays on the modern history of Switzerland: A book edited by Manfred Hettling et al. and published in 1998 [38] provides a selection of essays focusing on the history of modern Switzerland. One of the essays focuses on neutrality, while some of the other essays with a different focus nevertheless provide valuable insights on neutrality.

Third, an article published by Alois Riklin in 1991 [5] defines functions and dimensions of neutrality that it derives from historic precedent. It is useful to analyse these functions and dimensions, in order to better understand the character and definition of permanent neutrality policy. Riklin attempts to define these functions and dimensions independently of a specific time in history, i.e., he defines these as fundamental functions, which neutrality has had throughout its history of over 200 years. The article is discussed in Subsection 4.1.3.

Fourth, a collection of essays was published by, Georg Kreis, an emeritus professor of Swiss history at the University of Basel², in 2007 [71]. It contains mostly reflections on more contemporary developments in neutrality policy by notable people, such as former Federal Councillor Micheline Calmy-Rey. The essays reflect on the usefulness of Switzerland's neutrality policy in recent years. Subsection 4.1.4 discusses these essays and extracts useful aspects for the taxonomy in Section 4.4.

4.1.1 Historic Overview of Events

The aim of this subsection is to provide a general overview of important dates and events with respect to Swiss neutrality. The dates listed are commonplace knowledge with respect to Swiss history. They may be found in many history books, for example in books by Hettling (1998) [38], Riklin (1991) [5], Kreis (20017) [71], and Kreis (2014) [17]. A comprehensive history of Switzerland is provided in a book by Arlettaz from 2014 [72]. An overview of events deemed relevant for Swiss neutrality is shown in Table 4.2. These dates have been selected in order to provide the reader with an overview of the developments relevant with respect to Swiss neutrality. The content of Table 4.2 is shortly discussed in the following paragraphs.

A starting point of the history for neutrality, which is agreed to by most scholars, is in 1815, when neutrality was formally imposed on Switzerland by the major European powers at the Vienna Congress. Two dates listed in Table 4.2 are before 1815. They

²See <https://europa.unibas.ch/de/ueber-uns/personen/professuren/georg-kreis/>

Year	Event
1481	Nicholas of Flüe, patron saint of Switzerland, is claimed to have said to not meddle “ <i>in foreign dealings</i> ”.
1515	The “ <i>Marignano Defeat</i> ” marks a turning point in the foreign policy of the Swiss states.
1815	Vienna Congress: Neutrality is imposed on Switzerland for reasons of geopolitical stability.
1847	Civil war (“Sonderbundskrieg”) in Switzerland.
1848	Foundation of the <i>Swiss Confederation</i> .
1856/1857	Mobilisation of Swiss troops against Prussia in the context of the “ <i>Neuenburgerhandel</i> ”.
1863/1864	First Geneva Convention and foundation of the International Committee of the Red Cross (ICRC).
1889	The <i>Causa Wohlgemuth</i> poses a challenge to Swiss neutrality.
1914–1918	Mobilisation and neutrality during World War I
1920	Switzerland joins the League of Nations and adopts a <i>differentiated</i> approach towards neutrality.
1938	Switzerland asks the council of the League of Nations to re-establish its <i>integrally</i> neutral status, as war in Europe is imminent.
1939–1945	Return to a more integral neutrality due to World War II.
1946–1948	Switzerland resumes diplomatic relations with Soviet Russia (abolished in 1918). Continuation of integral neutrality due to the upcoming cold war.
1953	Switzerland as a country of the NNSC at the intra-Korean border.
1961	Switzerland is mandated to represent US interests in Cuba.
1980	Switzerland is mandated to represent US interests in Iran.
1989	End of the Cold War: Switzerland needs to rethink its role as a neutral country.
1992	The Swiss refuse to join the EU in a referendum, opposing the recommendation of their government.
2002	Switzerland joins the United Nations.
2005	Discussion on <i>active neutrality</i> following Federal Councillor Micheline Calmy-Rey’s statements.
2014	Crimea is occupied by Russia, which is condemned by Switzerland as a breach of international law.
2022	Russian attacks on Ukraine: Switzerland joins the economic sanctions against Russia and Swiss minister Ignazio Cassis coins the term of “cooperative” neutrality.

Table 4.2: Significant dates for the history of state neutrality in Switzerland.

are displayed with grey background. The listed events before 1815 are often mentioned when discussing the history of neutrality but they are (nowadays) rarely considered historically connected to neutrality. The events at said dates were often used as a justification for politically motivated claims to neutrality as a centuries-old, inherently Swiss characteristic in the 19th and early 20th century.³

In 1481, Nicholas of Flüe, the patron saint of Switzerland, provided council, which led to the Treaty of Stans and settled a conflict among cantons of the Old Confederacy. It is claimed that he said to not meddle “*in foreign dealings*” on this occasion, as is recorded in a chronicle from 1537.⁴ This is often used by neutrality ideologists as a justification for a historic claim to neutrality that reaches further back than 1815. However, the accuracy of the claim and its relevance for modern neutrality is strongly disputed by contemporary historians: First of all, the accuracy of the accounts about Nicholas of Flüe and his attributed statements are difficult to historically verify. Second, his attributed statements were about “not meddling in foreign deals”—while this might suggest the idea of remaining neutral, the foreign policy of the Old Confederacy did not strictly follow anything similar to modern neutrality policy; nevertheless, it may be considered one of several starting point (together, for example, with the Marignano Defeat discussed in the next paragraph) of a historical development that ultimately led to something like a de-facto military non-interference. Ultimately, neutrality was imposed on the Swiss in 1815, it was not necessarily something the Swiss would have chosen as a concept for themselves at that time due to the foreign policy restrictions the concept also brings about.⁵

1515 marks an important change in the foreign policy of the cantons of the Old Confederacy: The defeat of the Swiss states at Marignano marks their retreat from great power politics in Europe. Even though Marignano has been used as an argument for the century-old “Swiss tradition” of neutrality in the 19th and early 20th century, it is nowadays considered an event which might have marked a change in the foreign policy of the Swiss cantons but was not the glorified starting point of Switzerland’s neutrality policy. Historians claim that neutrality at that time was considered something negative, since it restricted the scope of actions.⁶

³See, for example, Georg Kreis’ comments in Arlettaz’ book from 2014 [72], or several essays outlined in later subsections released in a monograph edited by Hettling (1998) [38].

⁴This is, for example, outlined by Kreis in 2014 [17].

⁵See Kreis (2014) [17] and Hettling (1998) [38].

⁶See, for example, Kreis’ comments from 2014 [17], or analyses in the monograph edited by Hettling from 1998 [38], or the book by Arlettaz from 2014 [72].

1815 is generally considered the starting point of the modern-day approach to Swiss neutrality policy. Switzerland was defined as a neutral country by the major European powers at the Vienna Congress, following the Napoleonic wars. It is a matter of discussion, whether neutrality was imposed on or chosen by the Swiss. In any case the major European powers declared that it was a European interest to keep this geostrategically important territory neutral (i.e., out of the influence of any major European power). The major European powers did not only recognise but also guarantee Switzerland's neutrality.⁷ Kreis [17] explicitly states that the guarantee of Switzerland's neutrality was not understood to include a right of intervention by an external power in Switzerland's affairs, even though Austria and Prussia thought differently in times when they perceived Switzerland's neutrality to be compromised.

The next dates mark the beginning of Switzerland's contemporary form of government: In 1847, a civil war broke out between liberal (mostly protestant, pro-federal state) and conservative (mostly catholic, anti-federal state / pro-federation of states) cantons, eventually leading to the foundation of modern-day Switzerland in 1848. The constitution of 1848 provided the basis for modern-day Switzerland, which no longer was a loose confederation of states but followed a similar model to that of the United States of America as a federal state.

The constitution of 1848 included neutrality as one of the characteristics of the state, but only mentions it parenthetically when defining the protection of neutrality as one among many characteristics to be protected by the Federal Council and Federal Assembly.⁸

The incidents of 1856 and 1857 around the "*Neuenburgerhandel*" (*Neuchâtel Crisis*) caused the first mobilisation and election of a general in post-1848 Switzerland (General Henri Dufour, who is also one of the founders of the Red Cross and the Geneva Convention). The background of the Neuchâtel Crisis was an attempt by royalists in the canton of Neuchâtel to (illegally) re-establish the King of Prussia as monarch of Neuchâtel by means of a coup.

In 1863 and 1864, General Guillaume Dufour and his friend Henri Dunant found the international body known as the "Red Cross" (*International Committee of the Red Cross*): In 1863, a conference in Geneva with representatives from various countries leads to the Geneva Convention of 1864. Switzerland, as neutral country and host

⁷More details are discussed in later subsections. See also the comments by Kreis from 2014 [17, 72] and Hettling from 1998 [38].

⁸These are preserved up to this day in the Constitution of the Swiss Confederation, articles 173 and 185.

to the conference, is defined as depositary state of the convention and the ICRC's foundation in 1864 is a direct consequence of the First Geneva Convention.⁹

1898 marks the year of a significant challenge to Switzerland's neutrality, which emerged from Germany: A German police inspector named *August Wohlgemuth* was found by the Swiss police on Swiss territory in *Rheinfelden*. He was apparently (illegally) persecuting and spying on German left-leaning politicians who had had to flee Germany due to the so-called *Sozialistengesetze*. Wohlgemuth was expelled from Switzerland, which yielded negative diplomatic responses from Germany. Switzerland relied on its neutrality, while Germany claimed that this was not the kind of neutrality Germany had foreseen for Switzerland.

This incident provides an interesting example of Switzerland's own interpretation of neutrality being questioned by a major power.

Further mobilisations of Swiss troops occurred during World War I and World War II: Between 1914 and 1918 pro-German General Ulrich Wille was elected as General of the Swiss Armed Forces. As outlined later, in World War I neutrality served the function of internal cohesion, since support for the belligerents of the war followed the ethno-linguistic intra-Swiss borders.

After World War I, Switzerland adopted a *differential* approach towards neutrality when joining the League of Nations in 1920: While it could negotiate to fully preserve its military neutrality, it agreed to implement economic sanctions decided by the league. However, the adoption of this new approach to neutrality was not undisputed and led to a shift in the centuries of isolationist tendencies in Swiss foreign policy.¹⁰ Further sources claim that the League of Nations was also seen as a means against Bolshevik uprisings against governments, as the aftermath of World War I had led to social unrest in many European countries including Switzerland.¹¹ Then Swiss minister of foreign affairs, Felix Calonder, stated in 1919:¹²

“There is only one way out of this chaotic situation where passions are being unleashed. Instead of the mechanical sort of balance of power which has obtained until now [since the treaty of Westphalia in 1648], there needs to be a moral balance, provided by the League of Nations. Peace between nations is a condition of social peace within states [...] Should

⁹See also the ICRC's website for further details, as accessed in 2016 [73].

¹⁰This is outlined in detail in an article on swissinfo.ch, written by Bradley in 2019 [74] and history books referenced later on in this section.

¹¹See an article published by swissinfo.ch [75].

¹²Calonder said so at a meeting with Swiss reporters on 2nd July 1919, as is outlined by Burnand in 2019 [75].

Swiss democracy really stand aside waiting for the inevitable explosion, and refuse to join the League of Nations? The atrocities of the Russian revolution and the terrible trials visited on other nations by the dictatorship of the proletariat – are these not enough?”

It is noteworthy that the Swiss government (and also the non-Bolshevik world community) did not consider the question of joining the league to be a matter of neutrality but rather a matter of facing the “red tide”.¹³

However, this approach towards neutrality had to be given up in 1938, when Switzerland asked the council of the League of Nations for permission to return to a more integral approach towards neutrality due to the imminent war. World War II was, in many aspects, a continuous test for Switzerland’s neutrality and provides interesting examples of how neutrality interacts with practical aspects during a large-scale international conflict. Discussions on the implementation of neutrality in World War II are available, for example, in the monograph published by Hettling in 1998 [38]. One of the major themes is that of pragmatism when upholding permanent neutrality or, more clearly: Neutrality is always a subsidiary to national security; a state that cannot credibly maintain its national security can also not maintain neutrality. Furthermore, while neutrality was formally implemented in a puristic, integral manner, there were pragmatic exceptions. For example, Switzerland expected the German attack in the West, which ultimately went through the neutral territory of Belgium towards France, to potentially go through northern Switzerland. For this purpose, General Guisan, the head of the Swiss Armed Forces at that time, had engineered a secret agreement with his French equivalent: If Switzerland was attacked, France would be tasked with defending Swiss neutrality alongside the Swiss troops. In terms of neutrality law, this is perfectly permissible: in case of a breach of neutrality law through a belligerent country, other countries are expected to support the re-establishment of a country’s neutral status. In this case, a collaboration with other countries is in-line with neutrality law. However, with respect to the stricter idea of permanent and integral neutrality, such an agreement, if not kept secret, would have presumably led to Germany questioning Switzerland’s neutral status. Furthermore, Switzerland had to respond to various pressures from the Axis powers: Switzerland’s at time’s questionable approach towards admitting (Jewish, Roma, etc.) refugees also

¹³See explanations by Burnand from 2019 [75], which also reference claims in Dodis [76], a research project publishing Swiss historic diplomatic documents and commentaries.

has to be seen on this background:¹⁴ While formally neutral, the Swiss government was very well aware that it was fully surrounded by Axis powers and that its defence concept of guerilla warfare from bunkers in the mountains was questionable in terms of success for preventing an invasion in the lower lands, where the most important Swiss cities are located. The foreign policy was therefore that of maintaining permanent neutrality, in an integral characteristic formally, in order to stay out of the war: The integral approach was a necessity due to the collapse and *de facto* irrelevance of international structures, most notably the League of Nations. Nevertheless, the Swiss government also had to agree to concessions towards the axis powers, e.g., transports of material through its territory—which was in-line with neutrality law—for which it was later criticised as having shown a too collaborative attitude. The neutrality policy during World War II, in this sense, is an interesting example due to the constant balancing of maintaining permanent, and even integral neutrality, with pragmatic decisions required in order to not yield a reason for an invasion by the axis powers. Nevertheless, the Swiss government remained committed to integral neutrality throughout the war: Even after the war ended, it insisted to remain neutral, which it was criticised for by the USA and even first was excluded from discussions of a post-war peace structure, which was for example implemented by means of the foundation of the United Nations. This might also explain, why Switzerland did not become a full member of the United Nations until 2002: The United Nations was, from the Swiss perspectives, founded as an organisation of the winners of World War II—it would have been the wrong signal to the international community with respect to Switzerland’s neutrality, if Switzerland had joined the “winners’ club” right away.

After the second world war, Switzerland maintained its integrally neutral status while ensuring that it could provide services for the international community: The offices of the successor of the League of Nations, the UN, were located in the home of its predecessor in Geneva. Switzerland also resumed diplomatic relations with Soviet Russia, which it had abolished in 1918 due to the Soviet threat of a world revolution, which, according to the Swiss government, also had manifested itself through Soviet support for the 1918 Swiss general strike.¹⁵

¹⁴It should also be noted, that while Switzerland’s refugee policy at the time might seem unethical viewed from now, many other countries had very strict refugee policies as well; not least the USA with its strict limitations the number of refugees per country or ethnicity.

¹⁵This is also discussed in one of the later subsections, as part of reflections on neutrality discussed in the 1998 monograph edited by Hettling [38]. A short summary is also provided in an article released by *Dodis* [76], a research centre publishing and commenting historic documents of Swiss diplomacy.

Furthermore, Switzerland received a mandate to represent US interests in Cuba (1961)¹⁶ and Iran (1980)¹⁷; after the end of the cold war Switzerland was also mandated with representing Cuban interests in the US. Most noteworthy, however, is Switzerland’s role as an observer and supervisor at the intra-Korean border, which it holds since 1953. Switzerland was chosen by the United Nations Command (one of the belligerents) for the Neutral Nations Supervisory Commission in Korea (NNSC).¹⁸

With the end of the cold war in 1989, Switzerland’s role as an integrally neutral country with isolationist tendencies became challenged: The collapse of the bipolar world order no longer seemed to justify a non-participation in major international political projects. As Kreis (2014) outlines [17], already in 1990, before the Gulf war, Switzerland joined economic sanctions, which had been decided by the UN Security Council. In the early nineties, the Swiss Federal Council wanted to join the EU but was voted down by a national referendum. In 2002, the Swiss populus ratified Switzerland’s membership in the UN. Kreis compares the situation to the 1920s and 1930s with the League of Nations [17], as is also done in an article by Bradley from 2019 on swissinfo.ch [74]: Similar arguments to the Swiss 1920 referendum on joining the League of Nations were also brought forward in the 2002 referendum on joining the UN. Thomas Ferst, a lecturer at the Swiss Military Academy, which is attached to ETH in Zurich, characterises the changes of Swiss neutrality and foreign policy as follows:¹⁹

“Up until the end of the Cold War, the official policy of Switzerland was security through autonomy. Then there was a shift to security through international peace promotion, and after 2000 it changed to security through cooperation”.

The quote above also shows how neutrality is not a competitor of national security interests, but rather a tool thereof. It even seems plausible that the specific form of implementation of (permanent) neutrality is a function of the respective contemporary state of international affairs and thereby of national security considerations.

The foreign policy principles outlined above undoubtedly also have an influence on the implementation of permanent neutrality.

¹⁶As documented by FDFA in a website article from 2017 [77].

¹⁷As documented by FDFA in a website article from 2022 [78]

¹⁸See the website of the Swiss Armed Forces on its mission for the NNSC [79], as accessed in 2022, for further details.

¹⁹This quotation is included in and has been taken from a report published by Bradley in 2019 on swissinfo.ch [74].

In the first years of the millenium, Swiss Federal Councillor and foreign minister, Micheline Calmy-Rey, provoked discussions with her *active* approach towards neutrality after several speeches and comments in 2005 and 2006 (see Section 4.2).

Already before the annexation of Crimea in 2014, the reemerging conflict between Western countries and Russia has led to further discussions. As a consequence, Switzerland joined severe sanctions against Russia. Switzerland’s foreign minister, Federal Councillor Ignazio Cassis, has attempted to coin the term “*cooperative neutrality*” in 2022, although less successfully than his predecessor Micheline Calmy-Rey.

4.1.2 Manfred Hettling: Eine kleine Geschichte der Schweiz

The book *Eine kleine Geschichte der Schweiz* [38], edited by Manfred Hettling and published in 1998, contains eight essays on historic narratives of modern Switzerland (i.e., from around Napoleonic times onward, when Switzerland for the first time took the form of a unitary state during the “*Helvetic Republic*” instead of being a confederation of states). It has been selected as highly relevant, since it covers a history-oriented approach towards various topics very specific to Switzerland. It provides multiple perspectives from different authors that also enlighten the concept of state neutrality. In the following, the findings and interpretations relevant to Switzerland’s neutrality are discussed with respect to the relevant points for neutrality. They are discussed in the order of appearance in the monograph.

Neutrality as a Distinguishing Feature for National Identity

This essay, written by the editor himself, culminates in explaining permanent neutrality as a distinguishing feature of the modern Swiss state, in contrast to the European integration of the other countries: The political values of neutrality, direct democracy and civic self-regulation emphasise the differences to other European democracies. Swiss neutrality has a particular internal functions for Switzerland in terms of self-determination and as a distinguishing feature from other countries, forming an essential characteristic of Swiss national identity.²⁰

²⁰Manfred Hettling describes the evolvement of a national idea of Switzerland within the Swiss political elites of the 19th century. The national identity of Switzerland is described as having developed through travels of the elites through the cantons of Switzerland. In contrast to the European trend of the time, the Swiss elites would stay within their own country for their educational travels, leading to the general motive of “us” against “the others” in Switzerland’s self-perception. The author also explains that Switzerland—or rather its cantons—functioned as a “political laboratory” for democratic ideas of the 19th century. An contemporary reason for not wanting to integrate into greater Europe is brought forward on page 19: the ideals of a unified Europe exists for Switzerland also within its national boundaries by means of the national integration of the cantons.

Neutrality, the Global Status Quo, and Self-Defence

This essay, written by Mario König, covers Swiss politics and society in the 20th century. It presents a fact interesting with respect to Switzerland's neutrality: As already outlined in the previous subsection, diplomatic relations with the Soviet Union (as successor of the Russian Empire) were abolished in 1918 because of concerns regarding potential socialist revolutions in Switzerland. Diplomatic relations were only reestablished in 1948.²¹ König interprets this as a manifestation of a conservative approach to any *status quo* of world politics or global structures, which manifests itself in Swiss foreign policy as a neutral country: The Soviet Union, with its internationalist and revolutionist threat to the world's order, was clearly upsetting this system in which Switzerland had found a role of its own. This thesis deduces that Switzerland's implementation of permanent neutrality does tend to support a structural status quo with respect to world politics. König further discusses Switzerland's foreign policy at the beginning of the Cold War with regard to neutrality: in 1953, Federal Councillor Markus Feldmann notes that "*Soviet Russian threats are clear. In case Switzerland wants to stay out of risk, it has to avoid any suspicion of being actively involved in Germany's rearmament*".²²

Two main principles of permanent neutrality are identified by König: First, the permanently neutral country tends to support a system of world politics where it maintains its neutral role and, therefore, tends to have a conservative approach towards world politics. This principle is a logical conclusion from the neutral country's aim to preserve its neutral status, which it has within the status quo of world politics—whereas a change of the status quo (e.g., a socialist world revolution) might also mean a change to (or diminishment of) the acceptance and role of the permanently neutral.

²¹The year 1948 is stated by König in his essay, although the previous subsection stated that diplomatic relations were beginning to be re-established as early as 1946. According to Dodis [76], 1948 marks the year when economic relations were also re-established.

²²König claims that during the Cold War, the feeling of national self-defence of the Second World War was revived. He argues that Switzerland fundamentally differs from other European states by the absence of an (aristocratic-)bureaucratic apparatus. This allows high regional and communal diversity and also yields a different perception of the ideas of the age of enlightenment and a very uncommon interpretation of the term "freedom": historically, Switzerland has always seen itself as a dwarf surrounded by geopolitical giants. The ideas of self-containment and neutrality are described as a logical consequence. In essence, William Tell's story reflects the national tendency to abolish any ideas related to a governor's rule or hierarchy. The Swiss had already abolished the idea of loyalty to a ruler at the end of the Middle Ages. The ongoing mystic battle would always be against the external (in the remembrance of bad experiences with foreign rulers) and against the upper hierarchies, the national myth being based on a principle of equality. The farmer is seen as a liberator and liberated from authority; the farmer is always citizen. The basic values of Swiss society are described as: freedom, equality, unity and national faith. König concludes that only reforms that embrace these values have ever been passed.

Second, the neutral country adapts its neutrality as a function of potential threats it faces: The Soviet Russian threat for western Europe at the beginning of the cold war pushed Switzerland as a permanently neutral country to an implementation of equidistance to both sides (and, therefore, to establishing diplomatic relations with the Soviet Union), despite being culturally and politically closer to the west. Integral neutrality and its isolationist tendencies were a necessity in order to credibly uphold neutrality's inherent requirement of impartiality. Hence, neutrality also serves a national interest of reducing exposure to potential threats by not belonging to an opponent block of any major power.

Neutrality Narratives: Self-containment and the Balance of Powers

An essay thereafter by Andreas Suter is fully devoted to neutrality and its modern history. Suter outlines how the myth of Switzerland's national Saint, Nicholas of Flüe, could be understood as the starting point of Switzerland's neutrality. Allegedly, Nicholas of Flüe said: "*We should not meddle in foreign dealings*" (i.e., foreign conflicts). However, Suter emphasises that this statement is not historically fully accounted. Suter analyses the different narratives of the history of Swiss neutrality: Some of them interpret neutrality policy as a smart self-containment, which helps avoiding being drawn into any international conflicts. Others, including Suter, claim that neutrality was not self-imposed but rather a consequence of the decisions and negotiations of the major European powers at the Vienna Congress in 1815.²³ As Suter explains, the 1815 declaration of neutrality was not chosen by the Swiss. Rather, it was defined by the major European powers of the time: Austria, England, France, Prussia, and Russia. Its purpose was to achieve a *balance of power*: No consensus was found to allocate the geopolitically interesting territory of Switzerland to an influence sphere of any of the large powers. Nevertheless, Switzerland had itself pushed for a neutral status as well. This intention had already been expressed during the Napoleonic occupation preceding 1815.

Suter emphasises that neutrality is not just a concept of the political elites of the country, but is also deeply rooted in the self-perception of the Swiss populus—a

²³Suter explains, how some historians claim that the tradition of Swiss neutrality goes back to the 1515 Marignano Defeat. While the Marignano Defeat does mark a turning point in Swiss foreign policy, it can hardly be described as the beginning of neutrality policy. As already outlined in previous subsections, also Suter finds that the 1515 defeat did end an era of ambitious foreign politics and territorial claims of the Old Confederacy. After 1515, an increasing tendency towards non-interference began, which culminated with the 1815 (externally imposed and internally endorsed) declaration of permanent neutrality.

motive, which has already been discussed previously. Suter also outlines how neutrality has been an important factor for national security, in that it has prevented Switzerland from being drawn into any major political or military conflicts of the 19th and 20th century. The Swiss populus supports the concept of neutrality by means of its conservative decisions in popular votes with respect to Switzerland's foreign policy: For example, memberships in international organisations have been approved very late and a number of civic organisations foster and propagate the idea of independence and neutrality being inherently related to one another, such as AUNS²⁴ or the Swiss People's Party²⁵ (SVP). Suter also discusses the fundamental differences between European and Swiss political developments, reaching back to times before 1515. His most prominent example, however, dates from the year 1998, in which Switzerland's army still ranked as the fifth-largest in Europe, only outranked in size by Russia, Ukraine, France, and Turkey. This clearly endorsed the idea that neutrality had to be armed, since a neutral country cannot rely on allies for national defence purposes. With the end of the Cold War, however, a new debate on neutrality has been started. At the time of the writing of the essay in 1998, an increasing number of Swiss citizens questioned whether neutrality was still a viable concept for modern times. After all, according to Francis Fukuyama history had ended²⁶ and a European (or even global) conflict seemed further away than ever before. Suter finally claims that neutrality might have to be defined in a flexible way. After all, it is true that the emergence of *active neutrality* (see other parts of this Chapter) did bring about a more flexible approach towards expressing official opinions on international disputes.

Apart from philosophical and theoretical considerations on neutrality, Suter also provides a very thorough case study on the development of neutrality since 1815. Particularly interesting are the challenges to neutrality during times of foreign conflict or in times of increased political pressure from foreign powers. Examples are the First and Second World War, and the *Causa Wohlgemuth*. The latter is the name for a series of diplomatic disputes between Germany and Switzerland in the 19th century: Switzerland was allowing political dissidents, such as the German Social Democrats, to act and move freely within its borders.

The underlying narrative is that permanent neutrality is flexible and operates within a certain range of possibilities. In times of global conflicts that affect the status quo of world politics (such as World War I and World War II), neutrality

²⁴See <https://auns.ch/>.

²⁵See <https://www.svp.ch/>.

²⁶Most readers will be acquainted with Francis Fukuyama's book from 1992 *The End of History and the Last Man* [80].

tends to be implemented in a more integral manner. In times of an established global political structure, permanent neutrality is used in a more flexible manner.

One example of this approach is the *Causa Wohlgemuth*. It occurred during a time when Europe was governed by the *Balance of Power*, which had been defined after the Napoleonic wars by the five major European powers of the time: Austria, England, France, Prussia, and Russia. Switzerland enforced its neutrality against German interests and protected German (social democratic) dissidents from German spies. This seemed possible at that time, since other European powers also guaranteed the neutral status of Switzerland and the Swiss government did, therefore, not need to fear a German invasion despite German threats. A further example is Switzerland's implementation of neutrality during the world wars: Switzerland imposed a very strict, *integral* approach with isolationist tendencies, which was also followed later during the cold war. Particularly interesting is Switzerland's neutrality policy preceding World War II: While first integrating itself into the new status quo of the League of Nations and agreeing to support economic sanctions decided by the league, Switzerland quickly returned to its integral neutrality, when it became clear that the league had failed its purpose. After World War II Switzerland took great care to not join the United Nations as a "winner's club" and only joined once the cold war was over and membership in the UN had become the standard for virtually all countries in the world, with a very small number of exceptions.²⁷

4.1.3 Alois Riklin: Funktionen der schweizerischen Neutralität

In his article on Swiss neutrality from 1991, Alois Riklin [5] constructs a theoretical framework on the *functions* of permanent neutrality, which he derives from an analysis of Swiss neutrality history. An illustration of his definitions of conventional state neutrality functions in Figure 4.2. Riklin furthermore explains along which dimensions conventional state neutrality can evolve—these dimensions are illustrated in Figure 4.3. The functions and dimensions are shortly explained in the following.²⁸

The most important function of neutrality at the time of the foundation of the modern Swiss state in 1848 and previously in 1815 (Vienna Congress) was *national*

²⁷Some further details are available in a paper published by the author of this thesis in 2019 [43].

²⁸These functions have also been analysed and presented in a 2017 paper by the author of this thesis in thorough detail, which was published at ECCWS [43].

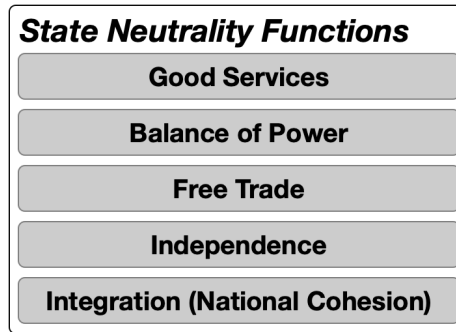


Figure 4.2: The functions of permanent neutrality, as defined by Riklin in 1991 [5].

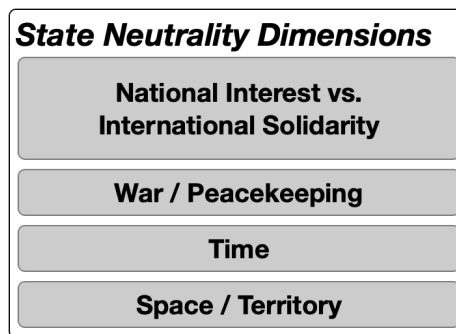


Figure 4.3: The dimensions for permanent neutrality, as defined by Riklin in 1991 [5].

cohesion. It is also referred to as the *integration* function. Due to the ethnic, linguistic, cultural and religious diversity of Switzerland, neutrality was a requirement for national cohesion. However, 1815 was not the first time this function of neutrality came into being. Previously, and in particular during the religious wars in Europe, Switzerland had adopted a policy of non-alliance and equality in terms of support for all belligerent sides, in order to prevent both an invasion and an internal split and civil war among the cantons. A further example of the importance of this factor was World War I: Support for the belligerents in the Swiss population was split across the ethno-linguistic regional boundaries. While the divide between the ethno-linguistic boundaries is no longer a threat to national cohesion today, a significant divide during referendums on contentious topics may still be observed. Hence, the national cohesion function, while no longer a matter of national security, is still important and might have the potential to regain its significance for national security—particularly in times of conflicts or tensions between neighbouring countries.

A further function of neutrality is that of independence—Riklin claims that neutrality is an important contribution for national independence, in particular independence from occupation or suppression, such as under Napoleonic France. During the

world wars and the cold war, this factor was seen as essential: Neutrality avoided the pressures states might be subject to in case they become a part of any specific block. Switzerland took great pride in being able to make its own decisions without having to adhere to the expectations of a specific block of countries.

Related to the previous function is free trade: Neutrality would also avoid, at least in its integral implementation, the full participation in one sole economic block of countries. In particular during the cold war, but also during times of the international isolation of the Republic of South Africa, Switzerland used neutrality as an argument for free trade with any country in the world. This would not necessarily mean that trade would need to happen with any other countries; but where in the Swiss interest and deemed acceptable by the majority of the population, free trade would be possible with any country, regardless of its affiliation to a specific block of countries, economic model, military alliance, or other interest group.

All functions outlined so far particularly benefit an implementing country of permanent neutrality. As outlined in the previous subsection, a requirement for neutrality is that also major powers support (or have an interest in) the neutral status of a country. Hence, it is reasonable that the remaining functions focus on the benefit of neutrality for the international community.

As already outlined previously, one main reason for declaring Switzerland's territory to be neutral by the Vienna Congress in 1815 was the establishment of a *Balance of Power* amongst the major European powers. Switzerland's territory, located centrally in Europe and hosting important passes through the Alps, was geostrategically interesting and would potentially provide any major power controlling it with the potential to significantly impact or even dominate any other major powers' interests. The geostrategically interesting position of Switzerland remains to this day. However, the potential of the surrounding countries to engage in serious conflicts or power competition with one another seems small—although this does not necessarily mean that this will remain so for all times. However, it is probably safe to say that, should Switzerland no longer be neutral, it would presumably be part of NATO and the EU as is the case with most surrounding countries—therefore, there would be no strategic advantage or quarrel over the status of Switzerland from a conventional Balance of Power perspective. However, there are other aspects, which are not directly related to Switzerland's territorial location, which might still be of interest from a Balance of Power perspective: On the one hand, Switzerland is a host country to a number of international organisations and forums. Furthermore, some global critical infrastructure, such as a SWIFT data centre, is located in Switzerland, along with international

research institutes, such as CERN. While there are a number of counter examples, where similar institutions are located in non-neutral countries (e.g., the UN in the USA, SWIFT data centres in Hong Kong, the USA, and the Netherlands), locating parts and specific branches of said institutions and organisations in a neutral country might nevertheless contribute to facilitating a Balance of Power between major blocks of countries. This view of the Balance of Power functions is inherently connected to the last functions of *Good Services*.

The most prominent function of a neutral country for the international community at the time of the millennium was that of *Good Services*—also known as *bona officia*. It manifests itself in services such as providing a means for diplomatic relations for countries that have severed their diplomatic ties (e.g., USA/Iran or historically USA/Cuba) or a role as neutral observer (e.g., at the intra-Korean border). Examples for these good services have already been discussed in the overview of Switzerland’s history in Subsection 4.1.1. As mentioned previously, Switzerland’s role as host country for international organisations, such as the United Nations, or its mediation in international discussions and conflicts, may be considered both a part of the Good Services function or the Balance of Power function.

Riklin also defines dimensions, as illustrated in Figure 4.3, which influence neutrality. These dimensions provide few insights in terms of a characterisation and understanding of neutrality but should be noted nevertheless, in order to understand which factors might influence a specific implementation of permanent neutrality.

First, neutrality changes over *time* and is defined with respect to some kind of *space*. Conventionally, the space relevant for neutrality is a territorial space: The geopolitical specifics of Switzerland’s territory were important when neutrality was first defined by the major powers of Europe in 1815; as mentioned it is less relevant nowadays. However, an implementation of space different to territory, such as cyberspace, might become relevant.

Additionally, neutrality fulfils its functions along the dimension of war and peacekeeping: In times of war, a neutral might be more strongly incentivised by a national interest of staying out of third-party conflicts and, therefore, neutrality might take a more isolationist form. Furthermore, Good Services might become more relevant, in order to enable communication between the conflicting parties, support refugees, and also allow a global financial system of some sort to exist in case of a world-wide conflict. In times of peace, cooperation might be more important and general measures for peacekeeping and prevention of conflicts and wars. This might also include a more active approach towards neutrality, where the neutral country, as trusted party, may

also prevent conflicts by specifically stating how international law should be applied in very clear cases.

Moreover, neutrality will always be subject to the tension between *national interests* and interests of the world community, here denominated by the term *international solidarity*. Examples in the history of Switzerland are numerous: For example, the questionable behaviour towards Jewish refugees during World War II, where it became a national policy to not admit Jewish refugees from Germany, developed under the pressure of the German government and the imminent threat of an invasion by the axis powers. Similar examples exist from the same time period concerning trade with or passage of goods of the axis powers. A country will always put its national interest of survival before the implementation of a puristic (or any other type of) neutrality—since the country can only be neutral if it still exists as a sovereign country. Therefore, neutrality could also be abolished in case it would be found that its consequences would be a direct threat to major national interests.

4.1.4 Georg Kreis: Die Schweizer Neutralität

A further collection of essays with a focus on Swiss neutrality has been published by Georg Kreis in 2007 [71]. The collection of essays has already been reviewed by the author of this thesis as part of a “CDT Mini Project” in 2017 [81], and the main points are drawn from that study.²⁹

Micheline Calmy-Rey provides her view on active neutrality in a foreword to the publication. She defines permanent neutrality as the commitment to not use military force for pursuing foreign policy goals and to only ever use military force, when under direct attack—therefore, it is a voluntary, perpetual guarantee for an abstention from using any kind of military force. Permanent neutrality may be understood as a commitment to being a messenger for peace.

Calmy-Rey confirms that permanent neutrality has to adapt itself to contemporary givens of world politics; isolationism, as was partially exercised during World War II or the Cold War, is not a founding principle of permanent neutrality *per se*, but was only a response to the geopolitical givens of those times. In order to preserve and advocate for peace and international law, Calmy-Rey infers that neutrality is by no means a synonym for indifference or complacency. By advocating for human rights and international law, Switzerland is not being partial in the sense that it would take the side of one or another party; Switzerland takes the side of international

²⁹Since the work on this “Mini Project” was conducted while enrolled as a DPhil student for this thesis, the work may be added to this thesis.

law. A secure and just international order is paramount also for Switzerland's own security and, therefore, also coherent with the country's national interest. The membership of Switzerland in the UN marked Switzerland's acknowledgement, that the UN's structures had advanced far enough to be understood as a generally approved global norm for peace and security. Calmy-Rey also reflects on a membership in the EU and the instinctive "no" that most Swiss citizens would answer to the question of whether Swiss neutrality would be compatible with a membership in the EU: The public perception is sceptical towards an obligation of solidarity Switzerland would have towards the EU, which might undermine Switzerland's neutrality. As is outlined in the next subsection, this exactly is the tipping point: It was the reason for the rejection of the concept of cooperative neutrality, which would have advertised a stronger collaboration with institutions, such as the EU or NATO. The rejection implies that cooperative would have been a too strong loosening of the ideas of permanent neutrality, which would have yielded a break with the norm of permanent neutrality as practiced so far. Therefore, it also provides an indicator for the limits of permanent neutrality practice.

Several of the following essays press the importance of a specific type of neutrality and rather have the notion of political campaigning, or they do not provide additional insights to what has already been discussed. Some of the authors of the essays in this publication are also the authors of previously discussed work. Since their main points have already been introduced and discussed they are not discussed a second discussion is omitted.

Paul Widmer's essay *Neutralität—eine Aussenpolitik mit Zukunft* ("Neutrality—a foreign policy principle for the future") looks onto the potential of neutrality from a post-Cold War perspective. He speaks in his capacity as former Swiss diplomat and ambassador, representing Switzerland in institutions such as the United Nations or the OSCE. He elaborates on the discrepancy between the elites and the populus on the topic of neutrality. While the elites are sceptical as to whether neutrality is suitable for contemporary times, it enjoys very broad support in Switzerland's population—the legal sovereign of Switzerland (this support will be further outlined in the next subsection). Widmer pleads for a more strict interpretation of neutrality policy for the future. According to Widmer, neutrality's most important asset is trust and credibility within the international community. He argues that assets have to be acquired during times of peace in order to be owned in times of conflict.

Widmer criticises Switzerland's participation in NATO's *Partnership for Peace* initiative and discusses the term *active* and *passive* neutrality. He outlines the seeming

contradiction between these two ideas. Neutrality, in its strict international law based definition (i.e., relative neutrality), is first of all a commitment to not participate in a conflict and to not pick a side—i.e. to be impartial. In this sense, it is first a decision to not take a decision and, as such, an act of passivity. However, the second notion of neutrality is that leading towards a decision: *A party is called upon to make a decision by acting as a judge, exactly because it is a neutral party. This denotes the active component of neutrality: It aims, by means of a dedicated foreign policy, to prevent, resolve, or reduce the impact of conflicts.* This is what is often denoted as the humanitarian tradition of Switzerland’s permanent neutrality. Widmer further states that, building on the tradition of humanitarian institutions and Switzerland’s engagement for international humanitarian law, the neutral is called upon to also voice concerns when international humanitarian law is violated:

“A neutral state should, of course, express itself on what has been widely accepted in principle by a broad consensus in the international community.”

Widmer finally emphasises, that the role of an impartial judge, which is exercised when implementing active neutrality, cannot be chosen by the neutral state itself. Rather, it has to be—formally or informally—mandated by the conflicting parties as a judge that is trusted by both sides. This outlines the principle of mutual support for the role of a neutral state and the international community, in particular also by conflicting parties and major powers.

4.2 Active Neutrality and Recent Developments

This section provides case study analysing discussions on the term of neutrality in Switzerland dating from the millennial decades up to 2023, in particular, with respect to Switzerland’s activities in foreign policy. The focus is on analysing, synthesising and, where appropriate, contrasting with previous findings, in order to further elaborate a systematic understanding of conventional neutrality.

The general temporal limitation of the case study coincides with Micheline Calmy-Rey’s time in office as a member of the Swiss federal government (the Swiss Federal Council): She took office on 1st January 2003 and resigned from her office 31st December 2011.³⁰

³⁰This information is available from the governmental website of the Swiss Administration [109], as accessed in 2017.

Date	Title	Source	Ref.
2003-11-14	Calmy-Reys Interpretation der Neutralität	NZZ	[82]
2005-02-12	Neutralitätsrhetorik und Sendungsgedanken	NZZ	[83]
2005-02-14	Neutralität – ein Verbrechen?	NZZ	[84]
2005-05-14	Den aussenpolitischen Kompass ausrichten	NZZ	[85]
2005-05-20	Mangelnde Kohärenz in der Aussenpolitik	NZZ	[86]
2005-05-20	Erweiterung der aussenpolitischen Pupillen	NZZ	[87]
2005-05-22	Calmy-Rey will weg von der EU-Fixierung	NZZ	[88]
2005-06-02	Erwartungen an die schweizerische Aussenpolitik	NZZ	[89]
2005-11-10	Aktive Neutralitätspolitik als Interessenpolitik	NZZ	[90]
2006-08-02	«Die aktive Neutralität ist nichts Neues»	swissinfo.ch	[91]
2006-08-22	Die Schweiz bald im Sicherheitsrat der UNO?	NZZ	[92]
2006-08-22	Plädoyer für eine noch aktivere Aussenpolitik	NZZ	[93]
2006-09-04	Calmy-Reys «aktive Neutralität»	NZZ	[94]
2007-01-17	SVP fordert Rückkehr zur passiven Neutralität	NZZ	[95]
2007-06-29	Schweiz als ehrlicher Broker	NZZ	[96]
2007-09-10	Calmy-Rey liebäugelt mit einem Sitz im UNO-Sicherheitsrat	NZZ	[97]
2007-09-11	Sitz im Sicherheitsrat als Ziel	NZZ	[98]
2007-10-06	Sicherheitsrat-Pläne stossen auf Ablehnung	NZZ	[99]
2011-09-13	Angriff auf Calmy-Reys Erbe	Der Bund	[100]
2011-12-31	Das war die Ära Calmy-Rey	Der Bund	[101]

Table 4.3: Listing of articles of the active neutrality debate.

Date	Title	Source	Ref.
2014-03-26	Standortbestimmung des Bundesrats im Ukraine-Konflikt	Press Release of the Federal Council	[102]
2014-08-13	Situation in der Ukraine: Bundesrat weitet seine Politik zur Vermeidung von Umgehungen aus	Press Release of the Federal Council	[103]
2021-01-21	«Die Schweiz und ihre Neutralität stehen vor grossen Herausforderungen»	swissinfo.ch	[104]
2022-07-14	Nachbefragung «Sicherheit 2022»: Kritischere Betrachtung der Neutralität, grösserer Pessimismus und stärkere Befürwortung der Armee infolge des Krieges in der Ukraine	Press Release of DDPS	[105]
2022-07-18	Babylonisches Sprachengewirr um die Neutralität	NZZ	[10]
2022-08-23	Mitmachen bei der NATO ohne Beitritt – geht das überhaupt?	Der Bund	[106]
2022-08-30	Zwischen Bourbaki-Szenario und neuer Rolle als Botschafterin der Freiheit: Eine selbstbewusste Neutralität bleibt im Interesse der Schweiz	NZZ	[107]
2022-09-07	Cassis wird neutralisiert – seine Bundesratskollegen sind nicht «kooperativ» und weisen den Neutralitätsbericht zurück	NZZ	[108]

Table 4.4: Listing of articles concerning Swiss neutrality following the Ukraine conflict.

During her time in office, Micheline Calmy-Rey was head of the Federal Department of Foreign Affairs (FDFA) and, as such, foreign minister of the Swiss Confederation. The scope of the case study is further limited to media coverage on the topic of the taxonomy and definition of Swiss neutrality policy—most commonly known during this time under the term of *active neutrality*. The case study is complemented by examples of further developments on the taxonomy and practice of Swiss neutrality policy, which emerged after the annexation of Crimea by the Russian Federation in 2014 and Switzerland’s subsequent practice of active neutrality, which culminated in the coining of the term of *cooperative neutrality* by the contemporary Swiss foreign minister, Federal Councillor Ignazio Cassis, in 2022, following the Russian invasion of Ukraine. However, the term cooperative neutrality, including its underlying concept, was rejected by the Swiss government, the Federal Council, in 2022 and the applied Swiss neutrality policy following the Russian annexation of Crimea in 2014 and the Russian invasion of Ukrainian territory in 2022 may be considered a consequence of the approach of active neutrality initiated by Micheline Calmy-Rey, as is outlined later in this section. The examples covered in this section from 2014 and 2022 may, therefore, be considered to be an annexe to the case study on active neutrality.

The sources considered for this case study are mainly drawn from the major Swiss newspaper *Neue Zürcher Zeitung* (NZZ), since its archives are the most substantial and easily accessible. Similar media outlets, such as *Tamedia* newspapers (e.g., *Der Bund* and *Tagesanzeiger*)³¹ and *swissinfo.ch*, have been found to be far less exhaustive on the topic and the news coverage is more or less identical to that of NZZ. Where the articles of Tamedia or swissinfo.ch do offer additional insights, these are explicitly listed and discussed. Further media outlets and official government publications have also been considered for this case study, although their number is far lower than the sources available in NZZ. An overview of all publications for the case study (including its annexe on the situation in Ukraine during and after 2014 and on cooperative neutrality) is listed in Table 4.3 (concerning the emergence of active neutrality) and Table 4.4 (neutrality after the Russian annexation of Crimea in 2014). The publications listed in Table 4.3 are discussed in Subsection 4.2.1 (concerning the emergence of the term *active neutrality* during Calmy-Rey’s time as minister of foreign affairs), Subsection 4.2.3 (on the compatibility of neutrality and obtaining a seat in the UN Security Council) and Subsection 4.2.2 (reflections published after Calmy-Rey’s re-

³¹See Section 5.3 for a thorough discussion on which media outlets are considered noteworthy sources for case studies in Switzerland.

Year	Event
2003	Micheline Calmy-Rey takes Office. She publicly expresses that an active, neutral foreign policy should be pursued.
2005	Basic principles of Swiss foreign policy are discussed during a retreat of the Federal Council.
2006	The discussion on neutrality gains momentum, as Calmy-Rey introduces the term “active neutrality”. She also suggests a discussion on the potential candidacy of Switzerland for a non-permanent seat in the UN Security Council.
2007—2011	Active neutrality establishes itself as a term and informs government practice.
2011	At the end of the year, Calmy-Rey steps down as a member of the government. This is not the result of political pressure.
2014	Switzerland condemns Russia’s annexation of Crimea due to its incompatibility with international law but does not join any sanctions. It does, however, implement the principle of “courant normal”, in order to prevent the circumvention of any sanctions.
2022	Switzerland condemns Russia’s invasion of Ukraine as illegal according to international law. Foreign minister Ignazio Cassis suggests the new approach of “cooperative neutrality”, which would result in strong military cooperation with NATO as a non-member country. The suggestion is dismissed by the Federal Council due to its incompatibility with permanent neutrality practice. Switzerland is elected by the UN General Assembly as a non-permanent member of the UN Security Council for the years 2023 and 2024 (Vide an article on FDFA’s website from 2022 [110]).

Table 4.5: Significant dates for the active neutrality debate.

signed from office in 2011 on her impact on neutrality practice). The publications listed in Table 4.4 are discussed in Subsection 4.2.5 and Subsection 4.2.6.

A chronological overview of the most important events with respect to recent developments and active neutrality is listed in Table 4.5.

4.2.1 The Emergence of a New Approach to Neutrality

A first presentation of Calmy-Rey's ideas on active neutrality emerged in a newspaper report of NZZ in November 2003 [82], the year Calmy-Rey took office. Calmy-Rey explained her idea of an active foreign policy for Switzerland and how this aligned with neutrality policy, which is not supposed to restrict Switzerland to a passive approach towards foreign policy. Rather, it is a matter of Switzerland's credibility and plausibility, as a neutral country, to speak up when international law is blatantly broken. While Calmy-Rey did not yet use the term *active* neutrality, she already spoke of an active approach to Swiss foreign policy and her statements already outlined what later came to be known under the term of active neutrality.

While Calmy-Rey's statement in 2003 already indicated the idea of active neutrality, the term and a thorough discussion only followed in 2005: Eight in-depth articles by NZZ, which were released between 12th February and 2nd June 2005 document the discussion and Calmy-Rey's definition of active neutrality as a term (see Table 4.3 for a listing of these articles).

A reflection by NZZ released on 12th February 2005 [83], which covers Calmy-Rey's recent travel to the middle east, discusses her idea of an "*active, neutral foreign policy*". The article speaks of a "diversification" of Swiss foreign policy, which used to be restricted mainly to foreign economic policy, and now follows a broader approach: It now also focuses on peace support and international human rights policy.

Furthermore, Calmy-Rey's view is presented, which criticises neutrality as having been far too long a limiting factor in foreign policy, used as a justification for isolationist tendencies. Calmy-Rey highlights neutrality as an opportunity for foreign policy, since it is a clear signal to the global community that Switzerland will always refrain, volutarily, from using military force as an instrument of foreign policy—so neutrality is predominantly a signal to the international community, which promotes peace.

Moreover, the permanently neutral has the advantage of being free from imperialist or colonialist history and, therefore, can more credibly take the role of an advocate for international law, human rights, and humanitarianism.

The article further reflects on the updated requirements for Good Services: It is no longer sufficient to only be impartial, which is the prerequisite a permanently neutral country provides. A mediator also has to “*provide means for pacification, reconstruction [...] excellent personal contacts to all parties and personnel and physical resources.*” [83].

Finally, the article draws an important conclusion, namely that neutrality policy, in whichever implementation, does not equal a neutrality of opinion or a neutrality of attitude. The article bases the conclusion on the aforementioned and the fact that Switzerland cannot exempt itself from a clear stance against international terrorism.

The article provides a number of important and interesting additions to the understanding of neutrality so far:

First of all, it explains why an active approach to neutrality is vital in the contemporary circumstances, since it is required in order to support the function of good services for the international community. Since the role of a neutral needs to not only be chosen by the neutral but also supported by a general consensus of the international community, it is vital that Switzerland adapts its foreign policy to a modern approach to neutrality, if Switzerland’s goal is a continuous acceptance of its beneficial role as a neutral for the international community.

Furthermore, the article extends the conservative approach towards neutrality, which was applied during the times of the cold war, and renews neutrality to a broader view on its possible implementations. Some of the statements in the article allow a connection to the previously discussed approach of Switzerland after World War I, when it joined the League of Nations and took an active role in supporting economic sanctions or even criticising the Soviet Union: There seem to be historic precedents that support the notion of active neutrality as an option within the possibilities of implementation of permanent neutrality.

The discussion on neutrality and its possibilities was continued in an article released in NZZ on 14th February 2005 [84], written by a guest author who is a professor in international law at the University of Zurich³². The author of this article presumably was Prof Daniel Thürer, since he matches all the points in the description of the author.³³

³²The author of this article presumably was Prof Daniel Thürer (University of Zurich), since he matches all the points in the author biography provided with the article. However, his name is not explicitly provided, so this remains an assumption. He is meanwhile an emeritus and his profile is available on the website of the University of Zurich: <https://www.ivr.uzh.ch/de/institutsmitglieder.html>

³³However, his name is not provided, so this assumption is unconfirmed.

The author elaborates on the history of and contemporary space for a correct implementation of neutrality. He builds his text on a quote by Israel Singer (then head of the World Jewish Congress) in the Financial Times earlier in the year: “Swiss ‘Neutrality’ in face of evil was a crime”. The author denies this statement, stating that the term neutrality is misinterpreted for other things that Switzerland did, out of a pragmatic sense of self-preservation, during World War II. He concludes that Switzerland did strictly adhere to relative neutrality during the war—and points out that also the USA were neutral, until Pearl Harbour had been attacked, and therefore would similarly have to have been labelled as criminal.

The author further implies that the concept of permanent neutrality is, in fact, a guarantor for peace: It states the renunciation of the use of force by the neutral and prohibition of any aggression for any third parties, and may be considered an ancestor of the prohibition of aggression in international law. In World War II neutrality enabled Switzerland to stay out of the war and maintain its democratic structures as one of very few countries in Europe. Neutrality enabled civil society, free press, freedom of art etc. to exist and even gave asylum to many refugees.

The author concludes that the world is different from 1945 and many of the principles of neutrality have become part of international law. He emphasises the difference of circumstances in different times, which shape the implementation of permanent neutrality, and lists four final principles paramount to the discussion on neutrality:

1. Security has become a common good under a collective responsibility;
2. “No state can stand wholly alone”³⁴, meaning that neutrality no longer implies the role of an outsider—it has changed towards the role of an impartial participant in a community of values and responsibility, who may function as a mediator, judge, consultant and “ami de tous”³⁵;
3. neutrality is a concept with respect to crises and conflicts and should, therefore, be understood as a broad concept for peacebuilding and conflict prevention;
4. neutrality evolved over a long time and particularly provides a high element of trustworthiness, which acts as an enabler for a very consistent and long-reaching foreign policy.

³⁴This quotation is referenced in the NZZ article [84] as having recently been stated by former UN General Secretary, Kofi Annan.

³⁵this quotation is attributed to Emer de Vattel in the NZZ article [84], who was a law scholar in the th century and instrumental to the development of the concept of international law.

Finally, the author endorses Micheline Calmy-Rey's approach, where neutrality is an opportunity for Swiss foreign policy to foster and promote a certain set of values in the international community.

4.2.2 Active Neutrality as Approved Foreign Policy Principle

The discussions on neutrality were taken further when active neutrality became an agenda item of the Federal Council, the collectively-led government of Switzerland. A quartet of newspaper publications document a meeting of the Federal Council on 18th May 2005, which would discuss this approach towards Switzerland's foreign policy and, consequently, also towards Calmy-Rey's approach towards neutrality.

A first article [85] was released in NZZ on Saturday, 14th May 2005, preceding the Federal Council meeting. This article anticipates the difficulty of the upcoming meeting of the Federal Council a few days before it took place: It sets the scene for the different views with respect to active neutrality and its potential criticism. It reiterates the main points of articles already presented and outlines how Micheline Calmy-Rey is attempting to push not only for active neutrality but also for a stronger coordination of Swiss foreign policy. The article explains how, historically, Swiss foreign policy has mostly been fragmented under the responsibility of individual diplomats. While an isolationist approach might be in-line with such an approach, it might no longer be compatible under the primacy of active neutrality, as arguably the post cold war era is no longer compatible with it: The world's contemporary complexities no longer allow a segmented approach towards foreign policy.

While the first article can only anticipate the points of discussion at the Federal Council meeting with respect to foreign policy and active neutrality, the remaining articles are set after it—two were released on 20th May 2005: One article in NZZ [86] explains how the Federal Council approved an approach with more coherence and coordination among the different ministries for Switzerland's foreign policy. It does not mention any denial of active neutrality by the collective government of Switzerland. The article emphasises a new clarity of communication by the Federal Council, which announced that the responsibility for leading Swiss foreign policy now lies with the Federal Council (as opposed to the historic approach to foreign policy as being purely segmented in terms of interests); the FDFA's role is defined as predominantly enabling options and making suggestions. The article does not explicitly mention the government's endorsement of active neutrality but does also not mention any rejection of it.

The other article in NZZ [87] released the same day focuses more on the opening of Swiss foreign policy beyond the European context but also implies an endorsement of active neutrality by the government. It focuses on the broadening of Swiss foreign relations beyond the European context: While the 1990s were predominantly focusing on the changes in Europe and the strongly evolving EU, a new focus beyond the EU and Europe has been decided by the Federal Council. Universality is mentioned as a traditional principle of Swiss foreign policy, which should again be stronger emphasised. The article also mentions that any suggestions and reports by Calmy-Rey had been endorsed by the Federal Council—while not implicitly mentioned, this also presumably means that the government implicitly supported Calmy-Rey’s active neutrality approach.

An article released two days later in NZZ [88], on 22nd May 2005, only confirms the stronger focus on global matters, while loosening the emphasis on European matters. Several readers’ comments released in NZZ shortly after [89], on 2nd June 2005, show that readers in general seem to support the idea of an active, open, foreign policy and even see it as a continuation of a tradition of neutrality and Swiss foreign policy:

- A first letter explains how a neutral actor might be particularly important, in order to be able to point the finger at the large powers’ misconduct in terms of international law (explicitly, the US imprisonment camp in Guantanamo Bay is mentioned), and how such a responsibility is particularly with Switzerland, as a depositary country of the Geneva Conventions. This remark is interesting also, when considering that in a multipolar world, most countries will belong to the influence sphere of one hegemon (see respective theory in Chapter 2 on IR theory) and, therefore, a neutral is required which may equally hold any hegemon to account, regardless of its affiliation.
- A second letter cautions to not misunderstand the changing focus of Swiss foreign policy towards global matters and, specifically, relations with the USA, as an endorsement of its foreign policy: It explains how the approach towards neutrality, as seen in 2005, is also a tactical step with respect to upcoming negotiations with the EU and that it does not mean a new closeness to other countries, such as the USA. Therefore, this letter understands active neutrality as a new form of more sovereign foreign policy practice, which also enables Switzerland to distinctly distance itself from the approaches of any major power.
- A third letter, finally, explains, how active neutrality and the traditional foreign policy approach of fragmented national interests are, in fact, compatible, since

the fragmentation is only a recent development and foreign policy, in particular in the sense of active neutrality, is always interests based. In fact, active neutrality is a national interests-focused foreign policy, since it promotes Swiss values and provides the neutral with a still vital role in a changed world—the letter therefore advocates for understanding active neutrality as a continuation of traditional foreign policy practice, albeit in a new, further developed way.

An article released later in the year [90], on 10th November 2005, picks up a very similar narrative as the third letter presented and elaborates further on it. It comments on recent speeches held by Micheline Calmy-Rey with respect to the new Swiss foreign policy and active neutrality. It emphasises that active neutrality is actually a direct following in the footsteps of the tradition of Swiss foreign policy being led by vital (defence and security) interests of Switzerland while following the principle of permanent neutrality. According to Calmy-Rey, neutrality should, in addition to its focus on supporting defence and security, be a means for supporting international law principles and helping to implement them. It is, therefore, vital to broadening the focus from the EU towards more collaboration with other “superpowers”, such as China, India, Brazil, Russia, and, in particular, the USA.

A further article [91], this time released in the news portal *swissinfo.ch* in 2006³⁶ and almost a year later, confirms that active neutrality is not *per se* a novel approach to neutrality but rather its adaptation to a changing world. This article further continues the narrative that active neutrality is not actually a new construct or a new invention. The authors include thoughts by Edouard Brunner, a former Swiss diplomat on the highest level. He explains how neutrality needs to adapt to the new world, where often states no longer fight conventional wars but find themselves in conflicts with armed non-state groups. All of this is set on the background and example of the conflict in Lebanon during those years: Switzerland, as the depositary state of the Geneva Conventions, is called upon to defend its values and to actively, with the advantages of being neutral (and, therefore, trustworthy for all parties), call out parties that fail to follow these conventions. Brunner specifically outlines examples from the cold war, where Switzerland took an official position by means of condemning, for example, the Soviet invasions in Hungary and Czechoslovakia. Ultimately, this news source and the expert it cites further support the narrative that

³⁶*swissinfo.ch* is the English language outlet of the Swiss Broadcasting Company *SRG SSR*, similar to BBC’s *World Service* it is supposed to provide independent news from a Swiss perspective to an international audience.

neutrality needs to adapt itself to its respective times and that its specifics alter over time.

It is noteworthy how consistent the comments on active neutrality are: On the one hand, active neutrality breaks with an isolationist (often labelled as “false”) interpretation of neutrality, which does not seem to rely on a long tradition but rather, in very uncertain periods in the past, seems to have been a result of the government’s perplexity, when faced with the complexity of a situation, and also a primate of non-interference when interference would have meant an unnecessary exposure with potentially fatal consequences. In this sense, isolationist neutrality seems like a pragmatic tool for respecting neutrality, while being incapacitated to respond in any other way than by minimal means or by silence. Therefore, a different (or more active) approach towards foreign policy (“*active neutrality*”) could appear contrary and mutually exclusive to the national interest of a country.

4.2.3 Neutrality’s Compatibility with a Seat in the Security Council

The discussions on active neutrality also brought about a follow-up discussion as to whether Switzerland could, with its tradition of permanent neutrality, become a member of the UN Security Council, or whether this would mean a weakening or even abandonment of permanent neutrality. It is useful to recall that Switzerland had only been a member of the United Nations since 2002 and, therefore, the confrontation with a potential (non-permanent) seat in the UN Security Council was indeed very new.

A total of seven³⁷ newspaper articles of NZZ, published between 2nd August 2006 and 11th September 2009 (see Table 4.3) cover this topic and the events and main points of contention with respect to neutrality are discussed in the following and contrasted with findings so far.

A front page lead [92] to an article [93] released on 22nd August 2006 documents how Micheline Calmy-Rey promoted not only an active neutrality policy and foreign policy for Switzerland but also, for the first time, launched the idea of a Swiss candidacy for a non-permanent seat in the UN Security Council.

The article [93] thereafter focuses on the contents of Calmy-Rey’s speech held at a meeting of all Swiss ambassadors in Bern (Switzerland) on the previous day. Calmy-

³⁷The articles listed further below and in Table 4.3 concerning a UN Security Council seat amount to eight. However, one article released on 22nd August 2006 is merely the front page lead for the second article released the same day.

Rey outlines the setting for her speech: The reality of a unipolar world, led by the USA, on the one side and the possible reality of a multilateral approach, as it is *de iure* defined by international law, which Switzerland supports. She further explains how a void exists between the expectations of the world towards the role of the EU and the reality of the EU's weariness in terms of international politics and foreign policy. The consequence is that Switzerland, not being a military or political superpower but being a neutral country, has to fully rely upon and promote the power and rule of (international) law. This is also the reason, why the Federal Council supported Swiss membership in the UN. Recent crises (Calmy-Rey was particularly referring to the Lebanon/Hizbollah-Israel conflict of 2006 and the War in Iraq of 2003) had shown that Switzerland's ability to effectively bring peace or other non-military solutions to conflicts was very limited. Calmy-Rey particularly criticised the strong overweight of NATO countries in the UN Security Council and saw Switzerland's role as a trusted neutral to be essential for a multilateral and international law-based approach.

Calmy-Rey also declares that international humanitarian law is weighed stronger than an orthodox, isolationist (or: *integral*) neutrality. Logically, this viewpoint makes sense, since relative neutrality itself relies on international law and, therefore, would become obsolete and difficult to defend in a world that neglects international law. In fact, a world that does not rely on basic international law would force Switzerland to rely more strongly on an isolationist interpretation of neutrality, in order to be able to maintain at least a minimum level of neutrality; it could even force a country to give up neutrality completely, in case major political and military powers no longer accept the international law basis for neutrality and, therefore, do not acknowledge a neutral status as being valid.

Shortly thereafter, a readers' reaction, which strongly criticises active neutrality, was released in NZZ [94] on 4th September 2006: Robert Blatter, the reader who wrote the comment, criticises that Switzerland only has economic but no political power in international matters and that it is, therefore, wrong to pursue an active approach to foreign policy. He claims that Calmy-Rey's active approach is, in fact, harmful and that her criticism of powerful nations on the basis of international law reduces Switzerland's credibility and trustworthiness as a neutral country.

While the comment is exemplary for a heated discussion on active neutrality and Switzerland's later decision to strive for an election to the UN Security Council as a non-permanent member, the content of the criticism seems rather weak: Calmy-Rey's argument, as outlined earlier, was exactly that because of the unipolar tendency of

international politics (with the USA as single “hegemon”³⁸) Switzerland’s role of a neutral was challenged and that Switzerland could only fulfil its neutral role in a world where multiple parties of some kind require a commonly trusted entity that should be neutral. Calmy-Rey suggests this to be a world in which international law and multilateralism are the pillars of world order—but it equally applies to the past, when Switzerland’s neutrality guaranteed a balance of power among the major five European powers in 1815, or in a bipolar world during the Cold War. The criticism in the article is, presumably, mainly aimed at the change in practice, which active neutrality brings about since Switzerland took a more passive approach during the Cold War or the World Wars.

Yet, as outlined, permanent neutrality is never a static policy but has to evolve along the changing givens of the international community—due to the changes at the end of the Cold War, the 1990s, and the increase in the importance of international terrorism and non-state actors brought about, it is clear that also permanent neutrality had to change. On the one hand, this change involved the change from a bipolar world to a unipolar world with the USA as the dominant hegemon, and potential new hegemon emerging. Furthermore, the change in the nature of conflict also shaped the changes in neutrality, as is clear from the newspaper articles already discussed: In the first years of the 21st century, conventional war seemed outdated, while non-state violent actors, such as armed political and terrorist groups gained importance.

The discussion and criticism continued, in particular in the following year (2007), which was a year of a general election of the Swiss parliament. An article published on 17th January 2007 [95] informs about the criticism of one of Switzerland’s major parties, the Swiss People’s Party (SVP), on active neutrality. The party is also represented in the Swiss government. The reasoning in the article does not provide a consistent case *per se* against active neutrality. It fails to outline, why active neutrality would be a breach of the tradition of the implementation of permanent neutrality.

The Swiss People’s Party argues in favour of a passive approach to neutrality and would like to extend a very passive interpretation of neutrality to any kind of conflict, i.e., to not only restrict neutrality’s strict definition to conflict between nation-states, as is the case in international law with relative neutrality, but to also apply it in an equal fashion to civil wars or conflicts between states and armed groups. Effectively, this would mean that Switzerland would not express its opinion on any international matters and restrict its foreign policy to only economic interests. While the Swiss

³⁸See Chapter 2.

People's Party voiced its intention to define neutrality in the Swiss constitution more precisely, it also acknowledged that it was difficult to find a fitting formulation for the range of what permanent neutrality means.

The opinion expressed by the Swiss People's Party needs to be understood on the background of the upcoming elections—in terms of reasons relying on historic precedent or a definition of permanent neutrality limitations, the arguments seem weak. While this article outlines the heated discussion around different approaches to neutrality that took place in Switzerland, it does not illuminate any reasons as to why a different approach to neutrality would not be allowed on the basis of historic precedent, and this reasoning seems to be missing completely in the reasoning of the Swiss People's Party.

The actual debate does not seem to be about neutrality *per se*, but rather about Switzerland's adaptation to a changed world. While the opinion of the Swiss People's Party does not seem to fully take into account the changes to world politics outlined previously, the argumentation for Calmy-Rey's active neutrality seems more coherent also and particularly when considering historic precedent with respect to permanent neutrality.

Later in 2007, a newspaper article published on 19th June [96] comments on several reports on neutrality, which were released by FDFA and presented by Calmy-Rey earlier in the year (although it is unclear, which reports exactly this refers to, as no reports have been found concerning neutrality on the website of FDFA dating from 2007). However, the article emphasises how Switzerland is not a “dwarf” in international politics but rather has been successful in its international initiatives (e.g., the establishment of a UN Human Rights Council). Calmy-Rey is cited as stating that neutrality is an asset for Swiss foreign policy, which allows Switzerland to act as a “*trusted broker*” for the international community—and thus emphasises the function of a trustworthy third party that a permanently neutral country should fulfil. It particularly outlines how Switzerland is not part of any specific “interest blocks” as a neutral country, as opposed, for example, to members of the EU, NATO, or other political or military blocks and interest groups.

The article also mentions how the term “active neutrality” is being avoided, due to its contentious potential. Most importantly, the article states again the option of candidacy as a neutral country for the UN Security Council as a non-permanent member. It picks up the first occurrence of this option during the stated speech of Calmy-Rey at a diplomat's meeting and elaborates how Calmy-Rey outlined that this option should be kept open prior to starting a discussion on its compatibility with

neutrality. The article states how other neutral countries (potentially less permanently neutral in the Swiss sense) have also been members and that this could be considered precedence for potential compatibility.

While an explicit discussion of any compatibility is avoided, it is noteworthy how the option of candidacy is upheld—even though from the point of writing of the article until an actual candidacy the article does state (and so does Calmy-Rey in the article) that a time frame of one or two decades would be required, until an actual candidacy could go ahead. Therefore, the actual candidacy cannot be considered an imminent personal goal that Micheline Calmy-Rey was striving for.

Only a short while later (the previous article was published on 29th June 2007, the current on 10th September 2007), an NZZ article [97] documents Micheline Calmy-Rey's further support and advocacy for a Swiss candidacy for the UN Security Council: It explains how Calmy-Rey now officially launched the process for a potential Swiss candidacy for a non-permanent seat in the UN Security Council, and how this was done only five years after Switzerland had become a member country of the UN. Calmy-Rey is documented as having outlined how the UN membership improved Switzerland's presence and trustworthiness in the global community. She is quoted to mention Switzerland's important role as a "bridge-builder" that does not follow a hidden agenda of interests due to its neutrality.

Calmy-Rey defines a timeline for candidacy in 2020 and emphasises the importance of a democratic discussion in Switzerland concerning this candidacy as soon as possible. She is also quoted as stating that Switzerland was 14th in the world in terms of its financial contributions to the UN and, therefore, should also take responsibility in the politics of the organisation accordingly.

In this sense, the article shows a number of themes already previously identified as manifesting themselves: Active neutrality as an approach which endorses neutrality as an asset for peacebuilding (here referred to as "bridge building") and Switzerland's duty as a neutral to be a trusted broker in international politics, which is not part of any specific interest block but at the same time has a moral-historic responsibility to uphold the ideas and values of the Geneva Conventions in particular and international law in general. Also, how this active approach benefits Switzerland since it ensures its continued international influence and role as a neutral country, instead of fading into insignificance due to passivity.

The next day (11th September 2007), a further article was released in NZZ [98], which documented the potential UN Security Council candidacy in a similar fashion. However, less than a month later, on 6th October 2007, NZZ also documents [99] the

refusal of the UN Security Council candidacy by several political groups and parties during parliamentary debates: First a parliamentary reflection on the five-year-old Swiss membership in the UN is presented: All major parties, apart from the Swiss People’s Party, see the membership as a success. The Swiss people’s party criticised that Switzerland did not have as much impact in the UN, despite paying a disproportionately large sum to the UN and its affiliated institutions. However, both the Federal Council and the parliamentary commission on foreign affairs draw a different conclusion and weigh Switzerland’s impact disproportionately when considering that there are 191 member states.

It is noteworthy and interesting that the Swiss People’s Party on the one hand criticises that Switzerland’s impact and importance in the UN is too low, while it also fundamentally opposes the active neutrality concept, which aims at a high influence in the UN and international organisations. With respect to the candidacy for the UN Security Council, the argument by Calmy-Rey in parliament was that measured by the amount of funds that Switzerland pays to the UN, its impact should be higher and so it should also become a non-permanent member of the UN Security Council. The Swiss People’s Party, however, criticises that Switzerland would have to state an opinion on decisions that impact international peace or conflict, which the Swiss People’s Party labels to be a “death sentence” for Swiss permanent neutrality. However, also other parties voiced concerns with respect to a UN Security Council membership.

4.2.4 Reflections in the Media after Calmy-Rey’s Resignation

Micheline Calmy-Rey, who introduced the term of active neutrality during her mandate as a Federal Councillor and minister of foreign affairs, left her office (formally: “resigned”³⁹) at the end of 2011. After she announced her resignation, a number of articles reflecting on her time and her achievements. The discussions from two articles are shortly presented in the following.

First a Tamedia article [100] released on 13th September 2011 reports that the *Aktion für eine unabhängige und Neutrale Schweiz* (AUNS) plans a vote on an amendment to the Swiss constitution, which would define Switzerland’s foreign policy practice at that time to be incompatible with neutrality and heavily restrict it. Apart from defining Switzerland’s neutrality to be “permanent, armed” [100], it would also define that the Swiss Armed Forces may not be deployed abroad, for example for peace missions. As is evident from the Swiss government’s website [111], as accessed

³⁹Swiss members of government usually remain members of government until they decide to step down—i.e., they formally have to resign. This is usually not the consequence of political pressure.

in 2022, the attempt by AUNS to submit this amendment of the constitution as a popular initiative and, therefore, make it subject to a vote, already failed when AUNS was searching for a sufficient amount of signatures.

As the article outlines, the constitution does not define any specifics of neutrality in terms of its implementation and also does not list it as a “raison d’être” of Switzerland; it has always been considered a flexible instrument of Swiss foreign policy. Indeed, as is discussed later and as has also been outlined by the author of this thesis in 2019 [43] and 2021 [3], the Swiss constitution does list the protection of neutrality as one of the duties of the federal government and federal parliament. However, it is not listed in the first articles of the constitution, where the foundational principles, structures, and ideas of the Swiss Confederation are defined. The article further explains how the initiative launched by AUNS aimed to specifically prevent a more active and flexible interpretation of neutrality, despite historic precedent legitimising a flexible approach towards neutrality. The article concludes, how this initiative by AUNS, which traditionally has strong ties to the Swiss People’s Party, is aimed specifically at undermining the developments in Swiss foreign policy under the Social Democrat Party (SP) Federal Councillor Micheline Calmy-Rey. The initiative, while marketing itself as an advocate of “real” neutrality, would have presumably reduced neutrality to an instrument of isolation from foreign policy initiatives. Even though this approach would probably be closer to the idea of *integral* neutrality as it was practised during the cold war and the second world war, it would unnecessarily tie the hands of the Swiss government: Precedents, for example from during the time of the First World War, exist, where Swiss soldiers had to protect the interests of Switzerland abroad since the countries within which they operated could not guarantee the safety of Swiss goods and personnel during the war. Even during the cold war or the Second World War, Switzerland was more active than AUNS would presumably want to acknowledge.⁴⁰

The second article [101], published on 13th September 2011, draws a holistic reflection on Calmy-Rey’s work as Federal Councillor and minister of foreign affairs, also beyond active neutrality. With respect to active neutrality, it states how Calmy-Rey framed and shaped the term and cites her once having said that the party which remains silent in situations of severe breaches of international law is not neutral.

⁴⁰ Apart from the historic events and precedents outlined in this case study, Hettling (1998) [38] and Kreis (2014) [17] provide further examples of Switzerland’s foreign policy activities and initiatives during the Second World War or Cold War. Another notable precedent is the Swiss reservations against a Soviet membership in the League of Nations, due to the inherent threat to the structure of the world (“world piece”) of Soviet and communist aims for a world revolution.

The article also lists several success stories, which indicates a positive *résumée* and application of the idea of active neutrality: First, the Swiss representation of the interests of Georgia and Russia in the respective other country following the 2008 conflict between the two countries is listed. Furthermore, the resumption of diplomatic relations between Turkey and Armenia in 2010 is mentioned, which resulted from Switzerland's active diplomacy with both countries. This illuminates how the *Good Services* component of neutrality is still important in contemporary times.

Both articles attest to the significant changes Clamy-Rey brought to Swiss foreign policy (and neutrality) with her new approach of active neutrality. In the same way, the articles also nicely denote, by listing historic precedents, how active neutrality builds on the historic continuity of the practice of neutrality policy, which always adapts itself to the world in which the neutral takes its role. In this sense, they support the idea that active neutrality is mainly an account and acknowledgement of the changes in world politics and the change in the nature of conflict already outlined previously.

An important conclusion from the analysis above is that neutrality, while following certain underlying principles, at the same time also requires adaptation to the World politics of its time, in order to maintain its significance.

4.2.5 Active Neutrality Following the Annexation of Crimea in 2014

This subsection and Section 4.2.6 may be understood as an annex to the actual case study on active neutrality. Even though the main focus of this subsection does not lie on the developments during the annexation of Crimea and the Russian war in Ukraine, the developments in 2014 and 2022 nevertheless provide important material, which underlines the significance of the emergence of active neutrality and also the limits of permanent neutrality in practice (i.e., where permanent neutrality limits a country in its foreign policy decisions, as will be outlined in Section 4.2.6).

In 2014, following the annexation of Crimea by the Russian Federation, the Federal Council of the Swiss Confederation responded with two public statements to the events. These are shortly introduced in the following. The Russian military operation for the occupation of Crimea is generally understood to have taken place from 20th to 26th February 2014, while the annexation happened on 18th March 2014.⁴¹

⁴¹See also a report by the RAND Corporation from 2017 [112], which offers a detailed outline on the events that took place with respect to the annexation of Crimea by Russia in 2014.

The first press release published on 26th March 2014 by the Federal Council [102] is a reaction by the Swiss government to the annexation of Crimea by the Russian Federation. It states that the Swiss government considers the annexation to be illegal since the government has found clear evidence that the annexation has breached international law. Furthermore, the press release outlines the government's intention to prevent any evasion of EU sanctions (or any other party's sanctions against Russia) through Switzerland. This is a practice which has already previously been applied in conflicts that were not following international law (e.g., the War on Iraq) and is known under the term "*courant normal*" principle⁴². The press release further documents the government's intention to actively support a diplomatic solution to the conflict between Russia and Ukraine within OSCE and by means of the Swiss presidency of OSCE during 2014.

A further press release [103], which was published by the Federal Council on 13th August 2014, reiterates Switzerland's handling of the annexation of Ukraine; namely that Switzerland attempts to ensure that sanctions cannot be circumvented through Swiss territory and that the Swiss Confederation considers the annexation of Crimea to be illegal according to international law. Furthermore, the "*courant normal*" principle is stated to have been extended to dual-use goods⁴³ and that the Swiss authorities had been instructed by the government to apply the rules very restrictively. The press release also states that the Swiss government further attempts to foster a diplomatic solution to the situation in Ukraine by means of the Swiss presidency in OSCE.

Both press releases and their contents document Switzerland's continued active foreign policy approach, in line with Calmy-Rey's vision of active neutrality: On the one hand, Switzerland does not pursue any direct involvement in the conflict and remains neutral from a military perspective. Switzerland does also not provide support one-sidedly for one of the parties in the conflict. Nevertheless, due to the undisputable evidence, which is available to the Swiss government, about breaches of international law, the Swiss government decides to issue a statement on the illegality of the annexation of Crimea by Russia. This approach is accompanied by the use of diplomatic means, in order to attempt to foster a diplomatic solution with both parties. This

⁴²This "*courant normal*" principle has been prominently applied by the Swiss government in 2003 as a reaction to the discussions around the legality of the War on Iraq by western countries, as has been documented by Bolliger in 2003 [113]. This was not the first time the idea of "*courant normal*" had been applied, as is outlined in the same article [113].

⁴³Dual-use goods denote goods that may be used for a military purpose but that are also traded for civilian purposes. This refers to further sanctions the EU had imposed on trade with Russia and Ukraine.

case provides an important precedent for the application of the principles and functions of active neutrality: On the one hand, the continued diplomatic relationship and negotiations with both parties, the call for a diplomatic solution, but also the clear legal position of the Swiss government due to the evidence and clarity of the provisions in international law. The assessment by the Swiss government is hoped to be understood as an impartial view of the situation, and, therefore, to provide a basis for negotiations between both parties. This case shows how a neutral country tends to be “on the side of international law” when international law and historic precedent provide the legitimacy and foundation for the role of a neutral country.

4.2.6 Neutrality Following the Russian War in Ukraine in 2022

In 2022, Russia invaded parts of Ukraine. This proved to be a challenging situation for the Swiss government with respect to neutrality and its definition. The minister of foreign affairs of Switzerland, Federal Councillor Ignazio Cassis, attempted to coin the term *cooperative neutrality* to allow for a stronger cooperation with NATO and western partners of Switzerland—the concept would have weakened some implicit principles of permanent neutrality, which is presumably the reason why the concept was dismissed by the Federal Council. In the following, some newspaper publications are discussed in order to outline the events that took place and put them into the context of the neutrality debate.

Preceding the Russian invasion in Ukraine⁴⁴, swissinfo.ch published an article by Bondolfi [104] on 21st January 2021 (so slightly more than a year before the invasion took place), which reflected on neutrality due to the increasing tensions between Russia and Ukraine. The article contains an interview with Micheline Calmy-Rey, outlining the challenges posed to Switzerland’s neutrality:

First, the interview reflects on the compatibility between a non-permanent seat in the security council and neutrality: Most security council decisions are political and not military, so there is no interference with relative neutrality *per se*: Calmy-Rey outlines how a seat in the Security Council enables Switzerland to take a more active position as a neutral country and to mediate between parties in a constructive manner, which is unique to a mutually trusted, neutral party. She points out the

⁴⁴The invasion began in the early hours of 24th February 2022 and has led to a war between Ukraine and Russia that has been evolving over the remainder of 2022 and beyond, as has been documented by any major news outlets, such as, for example, by CNN in an article written by Murphy in 2022 [114].

precedent of (then neutral) Sweden, which has used its seat in the Security Council in a similar fashion.

Calmy-Rey further emphasises the importance of a coherent and trustworthy foreign policy in support of its role as a neutral country, which consequently requires coherence of foreign policy, neutrality, Switzerland’s humanitarian tradition, and advocacy for adherence to international law.

Furthermore, it is stated how Switzerland’s strong adherence to principles of permanent neutrality is a matter of historic development and precedents. While international law on neutrality only applies to international conflicts between states, the principles of permanent neutrality as a state policy always adapts to the contemporary geopolitical givens: They need to be aligned with national, security, and foreign policy interests and the status quo of the structures and norms of the international community. Calmy-Rey explicitly defines active neutrality as *“being on the side of international law, not on the side of either or another party of a conflict. Of course, it is appropriate to express [the Swiss government’s] views and to condemn violations of international law. Remaining silent does not suffice.”*

Calmy-Rey also comments on suggestions that Switzerland should abolish its neutrality and become part of NATO, given the threat western countries are facing. Calmy-Rey outlines that neutrality faces major challenges, as does the collective security system of the UN, due to novel forms of conflicts. Moreover, Calmy-Rey outlines how armed neutrality is essential for Switzerland in order to remain independent from alliances and to maintain a credible ability to defend its own territory. She concludes that while neutrality is facing challenges, it is an essential asset for the special role Switzerland wishes to take in the international community, in order to provide good services, humanitarian engagement, and a significant soft power capability and that it is an instrument for diplomatic engagement and peace support. In that sense, it aligns with Switzerland’s national interest to promote international peace and stability, which are essential for a small state’s ability to interact globally (e.g., economically and politically).

A few months after the invasion, an article released in NZZ on 18th July 2022 [10] reflects on the many adjectives that have been applied to neutrality over time. It quotes Swiss foreign minister Marcel Pilet-Golaz during World War II, who stated that neutrality policy always adapts to international developments and events. The discussion on neutrality up to 2022 is stated to evolve around the adjectives of integral, differential, active, traditional, and cooperative neutrality—with further (but less prominent) adjectives existing. The article refers to research that characterises

the foreign policy exercised during World War II and the Cold War as “*integral neutrality*”, which started after Switzerland withdrew from obligations under the League of Nations in 1938. The article mentions how nowadays this would be equivalent to Switzerland distancing itself from the UN, while not abolishing its membership (also in 1938 Switzerland did not formally leave the League of Nations). *Differential* neutrality is mentioned to have evolved around 1920 after Switzerland joined the League of Nations and agreed to follow any economic sanctions of the league, while not being required to follow military sanctions. The article states that this is comparable to the status quo in 2022 with the UN. However, Switzerland has also agreed to support economic sanctions passed by the OSCE⁴⁵, which may be one of the distinguishing features of active neutrality.

Ignazio Cassis’ rejected idea of *cooperative* neutrality⁴⁶, which has only emerged in 2022, is described as an acknowledgement of the contemporary complexity of defending Swiss autonomy due to the changes in global security and an endorsement of a strongly cooperative approach in a highly interconnected and globalised world. In that sense, the cooperation would focus on states that share the same values of democracy, a rule-based international order for peace and human rights. This concept focuses on a stronger collaboration with partners like NATO, while not joining them—however the idea of cooperative neutrality has been dismissed by the Federal Council, presumably because it would signify a fundamental deviation from any permanent neutrality practice in the past: It would go beyond the mere promotion of international law and peace and involve an active focus on collaboration with a specific block of nations with respect to defence and security. In this sense, while not formally becoming a member of a military alliance, it would establish a formalised unidirectional collaboration with an alliance and abolish Switzerland’s full independence. Finally, active neutrality is characterised as the idea that Switzerland should not remain a passive observer of developments in the world but actively engage its trump card as a neutral country in order to work towards peace and stability in the world by means of humanitarian/good services. Also the foreign policy following World War I (“differential neutrality”) had been described as active by Marcel Pilet-Golaz at that time. The article from 18th July 2022 concludes by stating the hypothesis that there are three neutrality options (integral, differential, active) for

⁴⁵The Organization for Security and Co-operation in Europe (OSCE) is an international organisation focusing on resolving security affecting Europe by means of diplomacy and trust-building. Its decisions are consensus-based and politically, but not legally binding, as is outlined on OSCE’s website as accessed in 2022 [115].

⁴⁶As documented in an NZZ article from 7th September 2022 [108].

Switzerland's future and that the fourth option of a military alliance (most likely NATO) would presumably be doomed to fail due to the lacking support by the Swiss people.

The latter statement is reasonable considering a statement released by DDPS on 14th July 2022 [105], which reflects on the public opinion in Switzerland in 2022 with respect to matters relating to neutrality and national security. It is based on a study [39] carried out by Szvircsev et al. at ETH's Centre for Security Studies (CSS) from 30th May–17th June 2022 on a representative sample of 1003 members of Switzerland's voting population (i.e., members of the population with the right to take part in national referenda and elections). The study finds that the Swiss population judges the global future pessimistically with respect to conflicts and Switzerland's security and, therefore, is leaning towards stronger cooperation with institutions such as NATO or the EU. Nevertheless, neutrality as a basic principle of foreign policy still finds wide acceptance with 89% of the population firmly supporting this principle. At the same time, support for cooperation with NATO has reached a historic climax, with a support rate of 52% and 27% of the population even supporting NATO membership. Up to 35% of the interviewees stated that they believe a European defence collaboration might bring more security. The results of the study are noteworthy since they show very strong support for and identification with the principle of armed neutrality. While also the tendency towards a stronger collaboration with NATO and the EU is evident, the support for neutrality outreaches it by far. These numbers might have led to the government's later decision to abolish Ignazio Cassis' plans for "cooperative neutrality".

A further article released in Tamedia newspapers on 23rd August 2022 [106] outlines the idea of cooperative neutrality more clearly and discusses Cassis' plans with respect to cooperative neutrality. It provides insights in order to distinguish cooperative neutrality from active (or differential) neutrality, and does so by discussing a non-public draft paper by Cassis on cooperative neutrality. As outlined, cooperative neutrality would involve Swiss participation in exercises and military manoeuvres that practise NATO-wide collaboration in case of an invocation of NATO Article 5, i.e., NATO's collective defence response in case a member state is under attack. This would mean that Swiss troops would participate in exercises abroad, which practise a NATO Article 5 response and that such exercises could also be conducted in Switzerland. However, the article also refers to a NATO general, Harald Kujat of the German Bundeswehr, who comments that joining NATO would not contribute to Switzerland's national security, since it would mean that Switzerland would automatically become

part of an armed conflict between Russia and NATO and that this risk is very real in the international constellation of 2022. The outlined practical implementation of cooperative neutrality would provide for a precedential breach of historic neutrality practice. While military exercises abroad are common in Switzerland, collaborating in manoeuvres exercising NATO Article 5 would imply that Switzerland would collaborate with NATO or that it would expect to collaborate in case of an invocation of Article 5. It could be understood as a significant step towards NATO membership and would, in that case, significantly harm Switzerland's reputation as an independent, autonomous country whose primary goal of military activities is self-defence if, and only if, under direct attack by a third party.

Yet another article released in NZZ on 30th August 2022 [107] provides a thorough discussion of cooperative neutrality by comparing it to principles that governed neutrality practice around the period of World War I. The article reflects on a statement by Nobel laureate Carl Spittler, which he made during a similarly challenging time in December 1914 after the beginning of World War I. Spitteler emphasised the need for a rationally based approach towards neutrality, as opposed to an approach based on emotions (which might be comparable to the approach by the Swiss People's Party in the early 21st century, exaggerating neutrality as a holy imperative of isolation upon which Switzerland's success is based). The article promotes the idea of "cooperative neutrality" and mentions five neutrality hypotheses based on Spitteler's speech and contrasts them to the status quo of international affairs in 2022:

1. *"Neutrality is a contemporary means of escape from upcoming tensions"*: In 1914 this was mainly a response to the tensions between Germany and France and the resulting inner tensions in Switzerland between the respective linguistic groups. The article sees parallels in debates in 2022 between neutrality isolationists and neutrality activists (in the sense of Calmy-Rey's active neutrality), although it fails to explain how neutrality is a means of escape from the neutrality debate—it could be understood as two poles in the country, one leaning towards criticism against Russia and promoting an alliance with NATO and the EU for national security purposes, and the other one advocating no sanctions against Russia and continued collaboration with it. Nevertheless, this argument seems slightly incoherent, when contrasted with the inner peace neutrality brought to the tensions between linguistic groups during World War I:

The 2022 tensions in the neutrality debate are based on mutually exclusive approaches towards neutrality and, therefore, neutrality per se—whichever way it goes—will not appease either side. However, the author's argument may

be understood as a suggestion to not fulfil either side's demands and seek a compromise. Cooperative neutrality could potentially be such a compromise. Nevertheless, already active neutrality provides such a compromise—while cooperative neutrality seems to lean strongly towards the idea of very strong cooperation with NATO and clear alignment with NATO and western interests. Under these circumstances, neutrality might no longer be perceived as such by non-NATO and non-western countries.

2. *"It is the interest of Switzerland to define itself as an open part of the free world"*: The articles outline Spitteler's conclusion of the situation in 1914 concerning "great power politics" (*"Realpolitik"* or *"Machtpolitik"*), where the right of the stronger applied. The article's author compares it to the approaches of Russia or China towards disputes in 2022, where military power is used as a means of justifying and enforcing interests. The author of the article states that Switzerland's decision to join the sanctions against Russia following the 2022 invasion of Ukraine is no longer perceived as fully neutral by some states. He argues that this should be a reason for Switzerland to actively communicate, promote, and explain its novel approach. This would avoid being confused with non-aligned states like Serbia, India, or Egypt, who tend to choose opportunistically to support one side or another based on their own interests and often against international law. This is a significant difference from neutrality used for advocating international law. He further argues that in the 19th and 20th century, neutrality was an instrument to protect the quite unique republican and direct-democratic "special case" (*"Sonderfall"*) of Switzerland. Nowadays, neutrality might be understood more as a means for protecting the values of the free world (and international law), by a country which is armed, sovereign, neutral, independent from alliances and able to protect its own interests.
3. *"The freedom of action of Switzerland as a globalised economic power remains a focus [of neutrality policy and foreign policy]"*: The author argues that Switzerland could be seen by NATO as a partner, which protects the alpine geopolitical space, similar to the role Finland and Sweden took as befriended nations of NATO in the Baltic Sea before they expressed interest in becoming NATO members. While Spitteler argued that Switzerland does not engage in high-level foreign relations, since if it would commit to an alliance or secret treaties with foreign powers this would mean the end of Switzerland, the author of the article identifies this as being different now due to the contemporary status quo. He

argues that the contemporary goal is to secure Switzerland's freedom of action and to protect a rule-based security and economic architecture, within which Switzerland has a defined role within the structures of international law. Free trade is an antagonist of political confrontation and Switzerland's special relations with China could help to prevent, for example, a blockade of Taiwan. However, in case China would attack Taiwan, Switzerland would similarly have to support sanctions. This comparison seems a little far-fetched, since Sweden and Finland are attempting to join NATO and, therefore, the comparison could imply that Switzerland's new cooperative approach is just a first step towards joining NATO. Therefore, the author's argument in favour of a cooperative implementation of neutrality seems incoherent with the goal of still being recognised as neutral in the contemporary status quo of world politics beyond the structures of the EU or NATO.

4. *"Switzerland's greatest threat would be a conflict among its direct neighbours. Neutrality, therefore, remains a vital interest of Switzerland"*: The author outlines that while such a conflict seems unlikely, it nevertheless is a possibility. Authoritarian regimes aim at dividing the free world. Switzerland, therefore, needs to be ready for a "Bourbaki Scenario": In 1871, French troops were forced to evade a defeat by Prussia by fleeing to Switzerland, where the troops of General Bourbaki were disarmed and detained in a humanitarian way, which was a precedent for Swiss neutrality practice. The author fails to further outline how this is applicable to contemporary challenges. The reasoning provided by him rather seems to be an argument against stronger cooperation with NATO, since Switzerland has to be ready also for the unlikely case of implementing its neutrality towards NATO countries on the background of the unlikely, but possible case of instability within NATO. Therefore, an active neutrality approach seems more reasonable than the ideas brought forward in the cooperative neutrality concept.
5. *"Cooperative neutrality is an acceptable compromise and provides Switzerland with a "marge de manoeuvre" in its role as mediating power"*: Switzerland's neutrality is unique (e.g., Austria and Sweden are politically bound by their membership in the EU), which is an opportunity for being an ambassador for the free world, if Switzerland defines itself as a culturally western, but in terms of international law neutral country. This reasoning by the author, again, rather implies that active neutrality is the correct and coherent approach in order to

maintain the role of a trusted mediator, who advocates for international law. In case Switzerland would increase its cooperation with NATO to the level envisioned by cooperative neutrality, it would lose its trustworthiness as an independent third party that merely advocates for international law in an impartial sense. Switzerland would lose its “*marge de manoeuvre*” for the rest of the world, if it would be perceived as part of the NATO or EU block, despite advocating an approach labelled as cooperative neutrality. Cooperative neutrality would merely become a label to justify an alignment with NATO countries while attempting to keep the “neutrality” label, which would become meaningless as a consequence.

The author further argues that Switzerland is free of a colonial or imperial past and, therefore, has a better relationship with the countries of the global south or as a neutral mediator, for example, between Russia and the west. Switzerland—as opposed to Turkey—does not follow a hidden agenda.⁴⁷ Finally, the author claims that cooperative neutrality is a compromise, while a self-confident and self-determined approach towards neutrality would presumably provide Switzerland with more strength. Therefore, it seems, as if the author is not fully convinced of the advantages of cooperative neutrality. In summary, the article seems to rather provide reasons as to why cooperative neutrality is not compatible with historic precedents of permanent neutrality so far, whether active, differential, integral, armed, or other.

An article released on 7th September 2022 [108] marks the end of the cooperative neutrality discussion and manifests Switzerland’s continuation of neutrality policy under the *active neutrality* idea, which is coherent with historic precedent: The article documents Cassis’ unsuccessful attempt of having his definition of cooperative neutrality sanctioned. It claims that one of Cassis’ goals with cooperative neutrality, apart from those already mentioned, was to loosen the export restrictions of ammunition and war supplies for countries that had bought these supplies from Switzerland. As such, Switzerland continues to forbid the export of military goods, which it has sold to third countries (such as Germany) into war regions (such as Ukraine)—as a consequence, Germany is still forbidden to provide military goods earlier acquired from Switzerland to Ukraine.

Finally, it is also noteworthy that Switzerland was elected as a non-permanent member of the UN Security Council for the years 2023 and 2024. This election

⁴⁷The author seems to neglect that Turkey also has an imperial past as successor of the Ottoman Empire and Russia even has maintained to some extent the structures of Russia’s pre-World War I imperialism.

took place on 9th June 2022, as a report on the website of the Swiss Administration documents [110] (accessed in 2022). Switzerland was elected with 187 out of 193 votes by the General assembly, with no “no” votes and only a very small number of abstentions, as has been reported by swissinfo.ch in 2022 [116]. As the Federal Department of Foreign Affairs states (2022), *“no country in the Group of Western European and Other States has been elected with a better result”* [117]. Furthermore, *“Under its Federal Constitution, Switzerland has a duty to contribute to the peaceful coexistence of peoples and the preservation of natural resources. Its first seat on the Security Council will enable Switzerland to fulfil this mandate even more effectively.”*. Therefore, Switzerland sees its mandate in the UN Security Council to be in line not only with permanent neutrality and, more specifically, the idea of active neutrality, but also to be in line with the goals of the United Nations. The candidacy goes back to Calmy-Rey’s last year in office (2011) when the candidacy was officially submitted to the United Nations, as is documented by FDFA on its website [117] (as accessed in 2022). It is, therefore, the consequence of the active neutrality debate and Switzerland’s adaptation of its neutrality policy to the status quo of world politics: The global structures of the early 21st century provide a role for an independent, impartial, armed, neutral state and advocate for the international law structures.

4.2.7 Main Case Study Themes and Conclusions

The previous subsections provided a discussion of newspaper articles around the concept of active neutrality and its main protagonist, Federal Councillor Micheline Calmy-Rey. The facts, reflections, and comments presented in the newspaper articles were critically commented on with respect to their (logical, historical, or factual) validity. The main findings and ideas are summarised and put into context in the following. Furthermore, some conclusions are drawn from the main themes of the study.

The main findings and themes of the study are identified as follows:

Lemma 4.2.1. Active neutrality is an adaptation to a new status quo. Active neutrality has evolved as a term from political discussions. It has been outlined how active neutrality emerged as a term framed by Micheline Calmy-Rey during the first years of the millennium and, in particular, after the beginning of the War on Iraq 2003, which had not been sanctioned by the UN Security Council and was considered illegal by parts of the international community. The term active neutrality gained acceptance, while also raising criticism and discussion, particularly in 2005

and the upcoming years. The discussion around active neutrality strongly focused on an adaptation of neutrality to the status quo of global structures and world politics—this was brought forward as a main argument in favour of active neutrality. Indeed, the legendary national ethos of a very restricting neutrality policy, as brought forward by actors such as the Swiss People’s Party, drew from times of instability, the threat of (conventional) war and major tensions between countries. This was on the background of World War II and the Cold War. During the 1990s the world developed into a more unipolar structure, with the United Nations acting as a nucleus for conflict prevention and peacebuilding between states. On the other hand, novel types of conflicts, mainly involving non-state actors, emerged, such as the dominance of international terrorism as a threat. Hence, it seems plausible that active neutrality is an adaptation to a new status quo. At the same time, several articles reflected on previous precedents, namely what is labelled differential neutrality, typically referring to the period when Switzerland integrated itself into the collective security structures of the League of Nations after World War I; Switzerland maintained a neutral status but followed economic sanctions decided by the league. Switzerland again adopted to the global status quo, when it withdrew from the commitment to following the league’s economic sanctions, since it became evident that the League of Nations had become dysfunctional shortly before World War II.

Lemma 4.2.2. Active neutrality is a tool for peacebuilding and conflict prevention or resolution. The articles discussed why neutrality is a tool for building peace, preventing conflict and supporting the resolution of tensions: On the one hand, Switzerland is an impartial and trusted party for most states in the world due to its history of permanent neutrality. Therefore, it can help to mediate and maintain a means of communication between conflicting parties. On the other hand, Switzerland’s long history of impartiality due to neutrality provides it with an implicit authority to “judge” on breaches of international law: As a neutral country, Switzerland does not choose a specific side according to any affiliations with a political or military interest group. It decides on the basis of international (humanitarian) law and, therefore, its conclusions and judgements in international conflicts might have a greater likeliness of being heard by both conflicting parties. Switzerland spoke out against the War on Iraq but it also held Russia to account, when its activities were breaching international law. While it may be claimed that these public “judgements” did not resolve these conflicts, they did provide a strong moral case against the parties affected, eventually leading to a stronger diplomatic component in these conflicts and increased attempts to work towards peace. Switzerland’s successful candidacy for a

non-permanent seat in the UN Security Council further presses how a neutral country may attempt to influence world politics towards peace building and conflict prevention by means of supporting and making use of established structures and norms. On the other hand, as a (geographic) “dwarf” state, it is in the vital interest of Switzerland to support international law and norms, since they also provide for Switzerland’s security and are a vital pillar for Switzerland’s role as a neutral country, which contributes to Switzerland’s national security as its neutral status enjoys general support from the international community.

*Lemma 4.2.3. **The armed status is still of vital importance under active neutrality.*** Several of the discussed publications emphasised the importance, also under the principle of active neutrality, that Switzerland maintains a credible ability to defend itself. In particular, when acting under the idea of active neutrality, where Switzerland does express its view on international law and norms applied to specific conflicts and tensions, it needs to ensure that it is not reliant on third parties for its national security. Therefore, a comprehensive ability of self-defence needs to be upheld.

*Lemma 4.2.4. **Cooperative neutrality defines the boundaries of active neutrality.*** As discussed, the idea of cooperative neutrality was dismissed by the Federal Council in 2022. It has also been discussed how cooperative neutrality would, in fact, break with several historic principles and ideas of permanent neutrality, since it would include military exercises with third parties on collective defence. It would include collaboration, which would clearly signal a string entanglement specific block of countries (NATO, the EU), apart from the upholding of generally acknowledged international law and norms included in active neutrality practice. As such, the principle of cooperative neutrality, its discussion and dismissal, defines the boundaries of active and also permanent neutrality. The reflections on cooperative neutrality have also illustrated how neutrality is still an essential foundation of Swiss identity, by means of respective surveys of the Swiss population, and how Switzerland’s idea of neutrality is incompatible with a strong collaboration with NATO or the EU.

*Lemma 4.2.5. **Trustworthiness, impartiality, and credibility are important pillars of permanent neutrality, which are developed over time. They enable a “judge” function, as envisioned by active neutrality.*** The discussions on active and cooperative neutrality have also shown how trustworthiness, credibility, and impartiality are important foundations for permanent neutrality and, in particular, active neutrality: Switzerland can only implement its vision of an active foreign

policy on the basis of trustworthiness, credibility, and impartiality, which, in return rely on Switzerland's history of neutrality. A neutral country can only practice an active foreign policy (in the sense of active neutrality) in times where the international status quo (i.e., international structures, such as the UN, in combination with international law and norms) provides for it to do so, and on the basis of the trust gained over time as a neutral country. This emphasises and strengthens the thoughts on permanent neutrality brought forward by Widmer (see Subsection 4.1.4) on the seemingly contradicting symbiosis of activity and passivity with respect to neutrality: Active neutrality can only be practised (given the required prerequisites of a global status quo) on the basis of the inherently passive nature of permanent neutrality, which does not pick a side *per se*. Active neutrality sides with international law and norms, not with countries or political/military blocks of countries.

On the basis of these themes and findings, a definition of active neutrality is provided in the following:

Definition 4.2.1 (Active Neutrality). *Active neutrality denotes a specific implementation of permanent neutrality, which emphasises an active component. It relies on a neutral's trustworthiness, credibility, and impartiality, which enables the permanently neutral to provide public judgements with respect to global conflicts and tensions on the basis of international law and norms. It is in the national interest since it emphasises a structure of international law and norms, within which the permanently neutral has a specific role, which is internationally accepted and maintained, especially by major powers. Its distinguishing features are an active foreign policy, potential membership in international organisations, specifically the United Nations, and it may stretch out to membership as a non-permanent member of the UN Security Council, in order to emphasise the neutral's influence in working towards peace, conflict prevention, and conflict resolution. It is (as is permanent neutrality in general) always armed, in order to maintain credibility for non-reliance in terms of self-defence. Active neutrality is limited by the distinguishing features brought up during the cooperative neutrality discussion; namely an extensive (military) cooperative with a specific block of nations that would no longer make the claim of full (military) independence and self-reliance credible.*

Furthermore, the definition of active neutrality and the previously discussed themes and findings of the case study on active neutrality provide some conclusions for permanent neutrality, which are listed and explained in the following lemmas.

Lemma 4.2.6. Permanent neutrality operates within a certain range. The boundary of active neutrality has previously been defined by means of some distinguishing features of cooperative neutrality. On the other hand, previous subsections have also discussed different implementations of permanent neutrality, such as differential, integral, or relative neutrality. Thus, also permanent neutrality operates within certain boundaries, which differently emphasise the active or passive component of neutrality.

Lemma 4.2.7. Permanent neutrality adapts itself to the status quo of international politics and contemporary global structures and norms. The analyses and discussions in this chapter have shown how permanent neutrality takes the form most effective for providing a service, which is in the interest of the international community and, in particular, also in the interest of (most) major powers. This lemma is further drawn from the active neutrality debate discussed earlier in this chapter, which also focuses on what role a permanently neutral can take, in order to maintain neutrality as a relevant factor for international politics *in the future*. It is in the vital interest of a neutral state to maintain neutrality as a relevant concept of international politics, in order to also be able to profit from its protective character. Historic precedents from previous subsections further support this conclusion, as permanent neutrality has evolved over time, e.g., from a mainly geopolitical focus (on the neutrality of Alpine key territory within Europe) to differential neutrality (in order to support international and collective peace and stability efforts in the League of Nations) over integral neutrality (during times where international structures were less reliable) to active neutrality.

Lemma 4.2.8. The role of the permanently neutral needs to be accepted and supported by the international community. The reasons for this lemma have already been outlined in the reasoning for Lemma 4.2.7. Inherently, a country chooses (relative or permanent) neutrality in order to avoid being drawn into third-party conflicts. In order for this neutrality to be maintainable in the long term, it has to also be in the interest of the international community and, in particular, major powers.

Lemma 4.2.9. Permanent neutrality is in-line with national (security) interests. Similarly to the previous lemma, the main reasoning for this lemma has already been provided in Lemma 4.2.7: As already stated, (relative or permanent) neutrality is chosen in order to not be drawn into third-party conflicts, and, therefore, to avoid the destructive effect of international conflicts and tension on a country. Therefore,

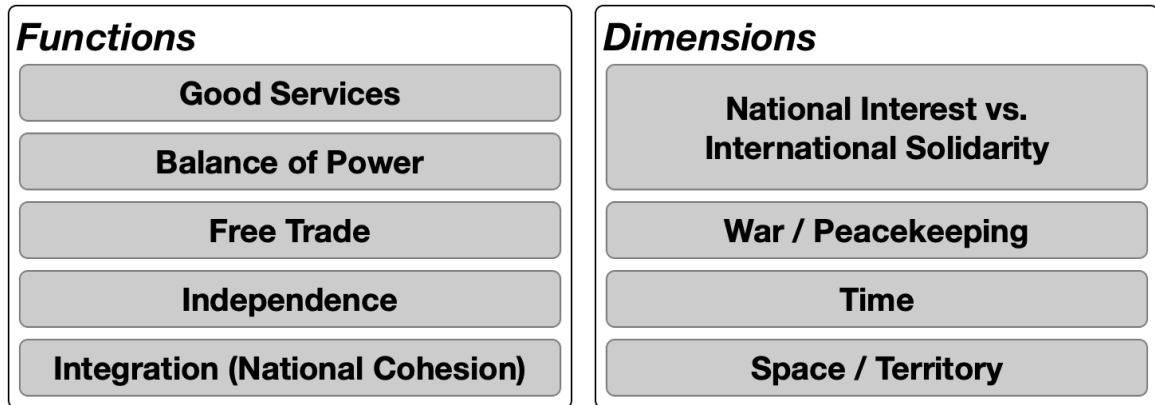


Figure 4.4: The functions of and dimensions for permanent neutrality, as presented in Subsection 4.1.3.

neutrality is always also subject to the national interest. In case a neutral status would infer significant risks to a country, it no longer aligns with national interests and would need to be abolished. This lemma is also supported by findings in this subsection and previous subsections, which show that neutrality while being contained in the Swiss Constitution, is not a founding principle of the Swiss state. Its inclusion in the Swiss constitution as a duty under the protection of the parliament and government is presumably also a consequence of the declaration and imposition of neutrality on Switzerland at the Vienna Congress in 1815, only slightly more than thirty years before the founding of the modern Swiss state.

4.3 Neutrality History: Main Themes and Conclusions

Apart from the lemmas stated in the previous subsection on active neutrality, some intermediate conclusions for permanent neutrality may be drawn by formulating the following lemmas:

*Lemma 4.3.1. Swiss neutrality is more specifically denoted by the term **permanent neutrality**, which relies on the definition of **relative neutrality**, denoting the military-focused international law definition of neutrality.* This follows directly from the discussions on neutrality in the previous sections.

*Lemma 4.3.2. Permanent neutrality operates within a range between an **emphasis of its active versus its passive components**.* This principle was formulated by Paul Widmer, as outlined in Subsection 4.1.4. Permanent neutrality has already been defined to operate within a certain range in Lemma 4.2.6. Widmer

outlined in the publication discussed in the case study, how there is an active and passive component to permanent neutrality. The passive component, inherent to neutrality not taking a decision, is a requirement for the active component, which is enabled by the trust in not picking any side with respect to a conflict, but at the same time allows promoting (and judging a situation according to) international law and norms.

Lemma 4.3.3. Different terms denote the location of a specific implementation of neutrality within and beyond the range of permanent neutrality, as outlined in Lemmas 4.2.6 and 4.3.2. In the case study on the history of Swiss neutrality, specific terms such as *relative neutrality* (also already outlined in Section 3.3), as well as *integral neutrality*, *differential neutrality*, and *active neutrality* have been extracted. They have been found to lie within the range of permanent neutrality; i.e., they all denote more specific implementations of permanent neutrality. These specific terms may be complemented by *military non-alliance*, *armed neutrality* or *geostrategic neutrality*. All these terms are defined later in Section 4.4.

Lemma 4.3.4. Permanent neutrality has been defined to serve certain functions and to evolve over specific dimensions. A reflection on functions of and dimensions for permanent neutrality has been provided in Subsection 4.1.3. The illustration of functions and dimensions provided in Subsection 4.1.3 is depicted in Figure 4.4 as an aide-mémoire.

Lemma 4.3.5. Permanent neutrality aims at facilitating a *Balance of Power*. Already the functions referred to in Lemma 4.3.4 define the *Balance of Power* function of permanent neutrality for the global community, in particular with respect to major powers. Furthermore, also Subsection 4.1.2 outlines the importance of neutrality for achieving a balance of power between the major powers of Europe during its imposition on Switzerland in 1815. While the approach in 1815 might have been focused on a geostrategic balance of power with respect to the military interest in Switzerland's Alpine territory at the centre of Europe, similar balance of power aspects are also relevant nowadays. These are mostly connected with the function of *Good Services*: Switzerland's neutral role as a depositary state of the Geneva Conventions, or its hosting of international organisations (e.g., the Red Cross and the UN), its non-permanent seat in the UN Security Council or its hosting of UN-accredited laboratories in Spiez for the independent investigation of Nuclear, Biological, and Chemical agents and substances (see an article on the federal administration's website, as accessed in 2022 [118], and Chapter 2) may also be considered to contribute to a balancing effect.

Lemma 4.3.6. Permanent neutrality is a tool for international peace, conflict prevention, resolution, and adherence to international law and norms.

Lemma 4.2.2 formulates how this applies to active neutrality. However, its generalisation to permanent neutrality more broadly also finds backing in the case study on permanent neutrality history: On the one hand, hosting international organisations, which are aimed at building a means of diplomacy for the international community in order to avoid military conflicts may already be understood as an argument in favour of this lemma: The hosting of the ICRC, UN, before it the League of Nations, as well as many further international organisations, but also treaties, such as the Geneva Conventions, are all inherently connected to Switzerland's neutrality. Already providing a space for such forums is a contribution to peace and conflict prevention. Further examples are good services provided by Switzerland, such as the representation of another party's interests in case there are no formal diplomatic relations established or Switzerland's role as a neutral observer on the intra-Korean border.

Lemma 4.3.7. Permanent neutrality is a commitment to refrain from using military force as a means of foreign policy and to strictly reserve military force for self-defence.

The case study on permanent neutrality outlined how several authors and actors see a definition of neutrality as a permanent commitment to not use any kind of military force as a means of foreign policy. For example, Paul Widmer provided such an argument, alongside with further authors, has claimed so in the publication discussed in Subsection 4.1.4. Looking at the history of Swiss neutrality, it is indeed evident that Switzerland has never used military force in order to enforce any foreign policy interests abroad. However, it has maintained a high capability to defend itself, in particular during the Cold War, as outlined in the next lemma.

Lemma 4.3.8. Permanent neutrality should always be armed, in order to uphold a credible level of self-reliance with respect to defence.

The analyses and discussions in this chapter outlined that permanent neutrality inherently has to be armed, in order to uphold a credible level of self-reliance. In particular, this is a distinguishing feature from cooperative neutrality, which would more strongly emphasise a reliance on partners with respect to exercising cooperative defence (such as in the case of the invocation of NATO Article 5) and potential collaboration in case of an attack. While this is not an explicit alliance, it may be characterised as an "alliance in case of an attack" and would contradict Lemma 4.2.5.

These findings contribute to what this thesis refers to as *conventional state neutrality theory*.

4.4 Conventional State Neutrality Theory

This section provides the pillars for understanding the main principles and definitions inferred from a historical and qualitative analysis of state neutrality practice, complemented by the findings on the legal definition of neutrality (*“relative neutrality”*). These findings are referred to as *conventional state neutrality theory*. They are supplemented by the implications that may be drawn for state neutrality in cyberspace subsequently in Chapter 5.

In order to define and outline conventional state neutrality theory, this section is structured as follows:

Subsection 4.4.1 provides an overview of the different “types” of neutrality by means of providing a basic taxonomy of the understanding of the different terms. The subsection defines these terms according to findings from previous sections.

Thereafter, Subsection 4.4.2 derives some conclusions, extending the basic taxonomy outlined in the previous subsection: Lemmas are formulated, which extend the basic taxonomy founded on fundamental definitions of neutrality types. These lemmas are also derived from the findings in the previous sections and provide a better understanding and a framework for understanding, discussing, and assessing new developments in the neutrality debates.

Subsection 4.4.3, finally, provides a model for conventional state neutrality, which lays the foundation for reflections on how conventional state neutrality theory may be extended to the cyber-era in later sections.

4.4.1 A Taxonomy: Neutrality Definitions

The aim of this subsection is to define different types of neutrality, in order to provide a basic taxonomy for neutrality theory—the definitions and the taxonomy are a major contribution of this thesis to the academic understanding of neutrality. The neutrality definitions are derived from various findings already outlined in previous sections. Definitions, which have already been made previously, are directly referenced here in order to provide a general overview.

As stated in Chapter 1, *Neutrality is first of all a philosophical term, which is applied to states in political science and international relations*. Based on the discussions, findings, and reflections in this thesis, the following definition of neutrality applies:

Definition 4.4.1 (Neutrality). *Neutrality* is a “policy or attitude between contending parties or states” and an “abstention from taking any part in a

war between other states”, characterised by the “state or condition of not being on any side”, or “impartiality”. This definition is drawn from the *Oxford English Dictionary* (OED) in 2022 [119].

A definition of state neutrality can be derived directly from this general definition of neutrality:

Definition 4.4.2 (State Neutrality). *State neutrality* denotes the concept outlined in Definition 4.4.1 when applied to states as actors in the international system of states (as understood in international relations theory).

Section 4.1 also discussed the term of *military non-alliance*, which may describe the status of Switzerland’s military and foreign policy following the Marignano Defeat of 1515, before neutrality *per se* came to be understood to be the concept of Swiss foreign policy. It is useful to provide a definition of military non-alliance, in order to understand its relation to state neutrality:

Definition 4.4.3 (Military Non-alliance). *Military Non-alliance* denotes the independence of a state from any military alliance system. It does not have a definition in international law and does also not restrict a state in terms of its participation in a conflict or support for conflicting parties. While it is not a type of neutrality *per se*, it may be seen as a prerequisite for neutrality: Only a state that is not part of a military alliance can also declare relative (or permanent) neutrality since it is independent of an alliance system that could trigger an obligation to support a specific side of a conflict.

The previous definitions are of a general character. In view of the findings in the previous sections, different types of state neutrality are defined more specifically in the following:

Definition 4.4.4 (Relative Neutrality). *Relative neutrality* refers to the definition of neutrality in international law, namely The Hague Conventions of 1907 (see Chapter 3). It is always relative to a specific conflict and does not require a continuous commitment to neutrality, apart from the commitment to neutrality towards the conflict relative to which it has been declared, hence its name. This aspect of neutrality has been thoroughly discussed in previous chapters. A later lemma formulates that relative neutrality is a prerequisite for permanent neutrality.

Definition 4.4.5 (Permanent Neutrality). *Permanent neutrality* denotes the commitment to relative neutrality for any potential conflict, even before such a conflict can be anticipated. This follows from Lemma 4.3.7. As outlined in Lemma 4.3.8 it makes sense to think of permanent neutrality as having to be armed, in order to fulfil the credibility of impartiality and self-reliance with respect to defence. Lemmas 4.2.5 to 4.2.9 and 4.3.1 to 4.3.6 further elaborate on the specifics of permanent neutrality.

In particular:

- Permanent neutrality operates in a range between a more active and a more passive implementation. Specific implementation forms have been given names, such as *integral*, *differential*, or *active* neutrality;
- permanent neutrality fulfils functions both for the country implementing it and the international community;
- it requires the general support of the international community, while not necessarily requiring the support of all major powers at all times;
- permanent neutrality relies on and contributes to a reputation of trustworthiness, impartiality, and credibility, which may enable a “judge” function in certain cases of international tensions and conflicts;
- it is in-line with national (security) interests and supports the status quo of established international governance structures, such as the UN;
- permanent neutrality contributes to a *Balance of Power*, international peace, conflict prevention and resolution, and adherence to international law and norms.

Both the terms relative neutrality and permanent neutrality are not created by the author of this thesis. Permanent neutrality is a term that has been used broadly in the neutrality discussion and also in literature specific to the history of state neutrality, as presented in previous sections.

Relative neutrality is a term used in a PhD thesis discussing state neutrality from a legal perspective and with a focus on Switzerland, published by its author Alexander Spring in 2014 [12]⁴⁸. As already outlined and referenced previously, it denotes the declaration of neutrality *relative* to a declared, armed conflict between third parties

⁴⁸See pages 36ff and pages 108–168 in Spring’s monograph [12].

in reference to the definitions of neutrality in The Hague Conventions of 1907 [54, 55]. The definition in this section is congruent with Spring’s idea of relative neutrality.

Spring also uses the term *permanent neutrality* and explains it from a legal perspective. Many of his findings are congruent with the definitions and lemmas formulated in this thesis. In particular, Spring explains that permanent neutrality is defined through “*customary international law and [...] dependent on a constant practice of permanently neutral states*”. The determination of its characteristics by means of historical case studies and an analysis of state practice, as has been done in the previous sections, is therefore a reasonable approach. Furthermore, several of the previously stated lemmas with respect to permanent neutrality are affirmed by statements made by Spring⁴⁹.

An important addition is stated by Spring and summarised in the following lemma:

Lemma 4.4.1. Permanent neutrality is compatible with participating in collective self-defence models, such as during the League of Nations or the UN under Art. 51 of the UN Charter. While Spring explains this primarily as a consequence of the formulation in the UN Charter, this conclusion is also derivable from historic precedent (and, therefore, customary international law), since Switzerland had also been a member of the League of Nations, while not giving up its permanent neutrality. Both precedents—membership in the UN and its consequences, as well as membership in the League of Nations—may be considered instances of differential neutrality, as defined later in this subsection.

The terms defined so far denote general ideas of neutrality, which are usually referred to when using the term “neutral” in connection with states. The terms defined in the following denote only specific subsets of neutrality. While the terms so far are often summarised under the term of “neutrality”, even though in one case this term may refer to relative neutrality and in another it may refer to permanent neutrality, the subsequent terms denote specific externalisations of what is referred to as “neutrality” and, therefore, are rarely subsumed under a general use of the term “neutrality”. Rather, they are mostly used in combination with the specific adjective, as defined in the following. The relation of the different terms to one another, including those already defined, is explained in the next subsection.

Definition 4.4.6 (Active Neutrality). See Definition 4.2.1.

⁴⁹See pages 39–40 in Spring’s monograph [12].

Definition 4.4.7 (Integral Neutrality). *Integral neutrality* denotes a specific form of permanent neutrality, which emphasises the passive component of the permanent neutrality range (see Lemmas 4.2.6 and 4.3.2). It is characterised by a renouncement of international political obligations (apart from neutrality) and omission of membership in international collective security organisations, such as the League of Nations or the UN. Political, economic, or military sanctions that are imposed by an international multilateral body are usually not followed under integral neutrality. A judge function is usually avoided unless specifically requested by parties of a conflict. The passive component features a (official) political distance from countries and organisations that form a part of any major power blocks and could potentially become part of a conflict. Integral neutrality is characterised by very strict adherence to the law of relative neutrality with respect to all countries, i.e., as if they were all at war with one another. In particular, integral neutrality relates to the implementation of permanent neutrality during World War II and the Cold War, as has been found earlier in this chapter. Integral neutrality is usually considered isolationist when considering political collaboration, although economic collaboration in the sense of enabling “free trade” is possible. Integral neutrality is usually implemented in an international climate, where the status quo of a global order is questioned and state neutrality as a concept experiences pressure and uncertainty in terms of its acceptance.

Definition 4.4.8 (Differential Neutrality). *Differential neutrality* denotes a specific form of permanent neutrality, which evolves around the central to the active component of the permanent neutrality range (see Lemmas 4.2.6 and 4.3.2). It is similar to active neutrality (See Definition 4.2.1), but is often used to refer to the specific implementation of state neutrality in the period between World War I and World War II, when Switzerland was a member of the League of Nations and adhered to economic sanctions decided by the league while refraining from participation in military sanctions. As such, differential neutrality ensures adherence to relative neutrality in case of a conflict, by not engaging in any military commitments while engaging in stronger political collaboration through participation in sanctions acknowledged by an international body. While differential neutrality and active neutrality may be considered similar or even equivalent, a differentiation may be drawn when considering that active neutrality also includes participating in sanctions decided by regional

bodies, such as the EU, and includes a stronger self-imposed component of the judge function.

Definition 4.4.9 (Geostrategic Neutrality). *Geostrategic neutrality* denotes the declaration of a territory/state as neutral based on geostrategic/territorial aspects, in order to facilitate a *balance of power* among major powers. It includes an emphasis on the neutral state's *independence* or *sovereignty* with regard to all major powers (in the sense of equidistance). Specifically, it denotes the definition of a specific geostrategically significant territory as neutral and, therefore, independent (or sovereign) from major political powers or blocks, in order to serve a common interest of all major powers in the territory while not granting any of it direct control. An example is the 1815 decision on Switzerland's neutrality. A similar case of geostrategic neutrality may be seen in Ukraine's nuclear disarmament and Russia's and the US' "guarantee" for its territorial integrity. While Ukraine's neutrality was also geostrategic, the common interest being the disarmament of a (new) nuclear power, it was less focused on the territory. The common interest lay in the management of nuclear weapons and, therefore, once the weapons were removed the assurance of neutrality was limited. Nevertheless, during the first years following the disarmament, Ukraine could have presumably relied on the guarantee. However, it failed to develop permanent neutrality from the original basis it received from geostrategic neutrality, which may be a reason why its neutrality ultimately could not be upheld and an armed conflict broke out with Russia.

Definition 4.4.10 (Armed Neutrality). *Armed neutrality* does not denote a specific form of implementation of state neutrality (or permanent neutrality) but is nevertheless a common term. It refers to the idea that permanent neutrality inherently requires a certain level of military self-reliance and, therefore, has to be armed. This idea has been explained in Lemmas 4.2.3 and 4.3.8.

Definition 4.4.11 (Cooperative Neutrality). *Cooperative neutrality* (as first described by Ignazio Cassis) denotes a foreign policy concept, which builds on a history of permanent neutrality and is characterised by a stronger military collaboration with a major military alliance and extensive political cooperation (e.g., by means of joining political and economic sanctions), in order to maintain the status quo of international politics. By doing so, however, it compromises the credibility and impartiality of classical

permanent neutrality considerations. It has emerged as a concept on the background of the Russian invasion of Ukraine (2022) and was put forth by the Swiss minister of foreign affairs, Ignazio Cassis, as has been outlined previously in this chapter. It has been dismissed by the Swiss government later the same year, due to its contradictions with some of the basic ideas of permanent neutrality.

4.4.2 Extended Taxonomy: Further Neutrality Lemmas

In the previous subsection basic definitions of different “types” of neutrality have been defined in order to provide a taxonomy of state neutrality and its related terms. The current subsection puts these definitions into relation to one another, in order to provide an extended taxonomy for state neutrality—this is a major contribution to the academic understanding of neutrality. Since this thesis is hosted in a department of Computer Science, logical operators are used for some relationships between terms, whose meaning is explained in the text. Although the use of these operators might seem unconventional in a social science setting, it is considered acceptable due to the interdisciplinary setting of this thesis.

The following lemma explains how definitions from the previous subsection relate to one another:

Lemma 4.4.2. The terms of the basic taxonomy outlined in Subsection 4.4.1 may be put into relation as follows:

military non-alliance $\supset$ state neutrality $\supset$ relative neutrality $\supset$ permanent neutrality

where “ $\supset$ ” is an operator stating that the right-hand operand is a part of the left-hand operand (“subset”) in the following sense: Any property of the left-hand operand applies to the right-hand operand, but not necessarily all properties of the right-hand operand always apply to the left-hand operand. One may also see this as follows: the definitions on the right-hand side are stricter than those on the left-hand side and, therefore, the cases which fall under the right-hand side definitions are subsets of the cases that fall under the left-hand side definitions.

This lemma follows from the definitions in the previous subsection: Military non-alliance is a prerequisite for any form of neutrality—legal and political or permanent. Similarly, relative neutrality is a legal codification of the more vague general idea of state neutrality and, therefore, is a more specific definition that might not cover all cases of the general idea of state neutrality. Permanent neutrality requires the

definition of relative neutrality to be applied to any potential conflict and, therefore, can only include a subset of the cases that are covered by relative neutrality.

Some definitions of neutrality mentioned previously have not yet been covered: Any implementation types of permanent neutrality (e.g., active neutrality) are treated in the following. Furthermore, armed neutrality is not really a specific type of permanent neutrality but rather a characteristic or prerequisite, so it has been omitted above and is treated later in Lemma 4.4.4. Geostrategic neutrality may be put into relation as follows:

Lemma 4.4.3.

geostrategic neutrality $\prec$ permanent neutrality

where “ $\prec$ ” means that geostrategic neutrality usually precedes permanent neutrality: Permanent neutrality may develop on the basis of geostrategic neutrality, but this is not a strict requirement.

This lemma is intentionally somewhat vague and has been added as a matter of completeness for Lemma 4.4.2; a full elaboration on geostrategic neutrality and its relation to (permanent) neutrality would be beyond the scope of this thesis.

As outlined, the term armed neutrality has been omitted earlier, since it doesn’t really denote a specific type of neutrality but rather a property of permanent neutrality, as is outlined in the following statement:

Lemma 4.4.4.

permanent neutrality $\Rightarrow$ armed

where “ $\Rightarrow$ ” means that the right-hand operand is a strict requirement for the left-hand operand.

This is a formally written version of Lemmas 4.2.3 and 4.3.8, which provide above statement in verbose form.

The following lemmas equally are formalised versions of previous lemmas:

Lemma 4.4.5.

passive past of neutral $\Leftarrow$ trusted active neutral

This is an extended and formalised version of Lemma 4.2.5: As formulated previously, a neutral power may exercise a judge function to a limited extent. The active component of neutrality, which provides for the judge function, strictly relies on a passive past, during which the neutral power gained trust.

Lemma 4.4.6.

$$\text{passive dimension} \sqsupset \text{integral neutrality}$$

where “ $\sqsupset$ ” is defined as follows:

Most of the right-hand operand’s properties are part of the left-hand operand.

This lemma is a formalised version of Lemma 4.3.2 and the comments and explanations included in Definition 4.4.7. Its main finding is that integral neutrality emphasises the passive dimension of the permanent neutrality range; i.e., many properties of integral neutrality are located on the passive dimension. However, as outlined earlier, this should not mean that no activities in the active dimension are possible; they are merely smaller in number than those on the passive dimension.

In a different notation, this finding could also be expressed as follows:

$$\text{integral neutrality} \equiv \text{passive dimension} > \text{active dimension}$$

Lemma 4.4.7. Similarly to Lemma 4.4.6, the following may be formulated for differential neutrality:

$$\text{active dimension} \sqsupset \text{differential neutrality}$$

This follows from Lemma 4.3.2 and Definition 4.4.8. As also in Lemma 4.4.6, this may also be expressed in a slightly different notation as follows:

$$\text{differential neutrality} \equiv \text{passive dimension} \leq \text{active dimension}$$

For matters of formal mathematical completeness with respect to the operator, differential neutrality shall also include cases, where the passive and active dimension are equally weighted.

Lemma 4.4.8. Similarly to the previous two lemmas, this lemma identifies the gravitation point of active neutrality on the range of permanent neutrality:

$$\text{active dimension} \sqsupset \text{active neutrality}$$

As outlined previously, historically active neutrality has emphasised the active component slightly more than differential neutrality. Therefore, the following notation of this lemma omits equality and uses a strict operand:

$$\text{active neutrality} \equiv \text{passive dimension} < \text{active dimension}$$

Nevertheless, as the next lemma shows, active and differential neutrality are considered to be functionally equivalent. These terms describe the same type of abstraction

with respect to a “type” of permanent neutrality during different times in history. The time to which active neutrality refers is defined by a slightly stronger occurrence of the active dimensions but both terms, in abstraction, refer to the same idea of implementing permanent neutrality.

Lemma 4.4.9. As already outlined, this equivalence of the terms is formalised as follows:

$$\text{active neutrality} \equiv \text{differential neutrality}$$

When used not to refer to a specific time in history, but rather as an abstract concept of implementation of permanent neutrality, these terms are interchangeable. When they are more practically related to the actual implementation, they are “almost” equivalent, with active neutrality having a gravitation point on the permanent neutrality range, which is located slightly further away from the passive dimension than that of differential neutrality.

Lemma 4.4.10. Finally, it is worthwhile to consider the compatibility of cooperative neutrality with the permanent neutrality range of permanent neutrality and formalise this relation. As shown in Lemma 4.2.4, cooperative neutrality goes beyond the boundaries of active neutrality and would also break with what is so far considered to be the limit of the boundaries of permanent neutrality. Nevertheless, it contains many considerations found in the active dimension of permanent neutrality. This is formalised as follows:

$$\text{active dimension} \simeq \text{cooperative neutrality}$$

where “ $\simeq$ ” denotes that cooperative neutrality is a “type” of neutrality, which is similar to the active dimension of permanent neutrality. The difference to active and differential neutrality is that there is a (complete or almost complete) lack of the passive dimension of permanent neutrality and that cooperative neutrality goes beyond what would usually be considered the active end of the range of permanent neutrality.

Figure 4.5 is derived from the above definitions and lemmas. It visually illustrates the findings on neutrality and its taxonomy. Figure 4.5 provides an overview of what is understood to be the state of *neutrality theory* as seen in 2023, i.e., *conventional* state neutrality theory—it does not involve cyberspace, since the aim of the current chapter is to provide an understanding of conventional neutrality theory. Adding the component of cyberspace to neutrality and deriving the impact of cyberspace on neutrality is the topic of Chapter 5.

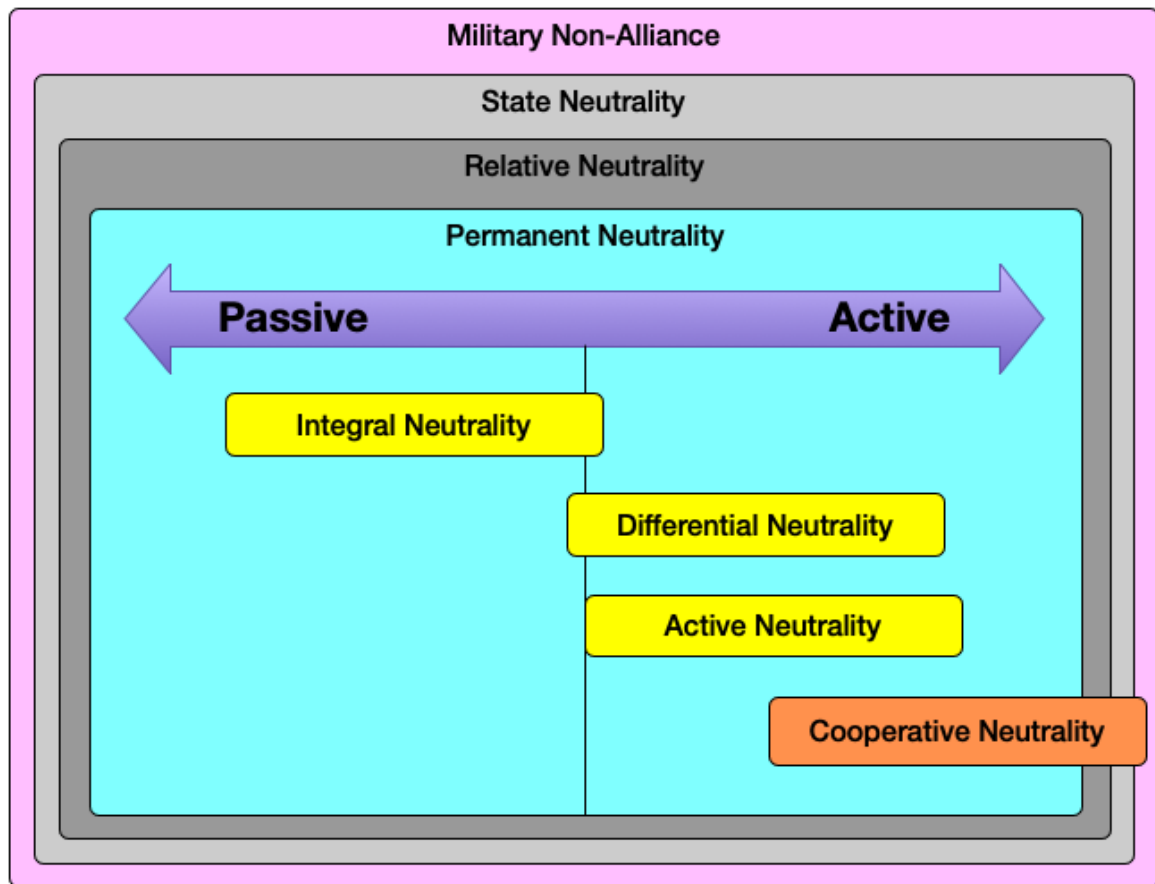


Figure 4.5: A visualised summary of the findings on state neutrality and its taxonomy.

As illustrated in Figure 4.5, military non-alliance, state neutrality, relative neutrality, and permanent neutrality have a “containing” relation to one another (see Lemma 4.4.2). Within permanent neutrality, the figure shows the range of its specific “types”, with a passive and an active dimension. The permanent neutrality types of integral, differential, and active neutrality are shown in relation to their location along this range. Furthermore, the figure shows that cooperative neutrality clearly breaches the range of permanent neutrality and, potentially, also the range of any other neutralities. The only limitation to cooperative neutrality, which is evident from case studies in this chapter, is that of a military alliance: It is, therefore, within the boundaries of military non-alliance but outside the boundaries of permanent neutrality and, potentially, also outside the boundaries of relative or state neutrality.⁵⁰ A

⁵⁰The rules outlined in international law that determine relative neutrality have already been discussed in the previous chapter. Some of the ideas outlined in the discussions around cooperative neutrality might potentially breach these rules, although it has always been the official view of the Swiss government that the main pillars of permanent neutrality (and therefore Swiss foreign policy) are those outlined in international law as relative neutrality, notwithstanding that there

thorough discussion of the specifics of cooperative neutrality beyond what has already been provided in this chapter is beyond the scope of this thesis.

4.4.3 Intermediary Conclusions for State Neutrality

So far, this thesis has provided a broad discussion and analyses on how historic precedents and legal codifications have shaped the understanding of what state neutrality is:

On the one hand, relative neutrality explains what state neutrality is understood to be, in terms of international law, relative to specifically declared conflicts. Relative neutrality has been mainly discussed in Chapter 3, including some intermediary conclusions with respect to cyberspace.

On the other hand, permanent neutrality is understood as a permanent commitment to act within the boundaries of relative neutrality in case of a conflict and to establish a practice of permanent neutrality during times of peace that enables this. This practice is defined by historic precedent and certain principles that have been outlined in lemmas. Furthermore, permanent neutrality may take different shapes depending on the international environment it is set in: Terms like differential, integral, or active neutrality have been extracted from the literature, discussions, and case studies.

Finally, a taxonomy was provided that provided an overview of all the definitions relevant to state neutrality theory. Further, an extended taxonomy (including formalised lemmas) was formulated, in order to provide a general overview of what conventional state neutrality consists of. These terms have been defined, put into relation with one another, and thoroughly discussed—this taxonomy of terms and relationships, as well as principles for permanent neutrality form an original contribution of this thesis for establishing a conceptual framework for conventional neutrality theory.

are also the *de-facto* limits to permanent neutrality outlined earlier, which have developed from historic precedent. Some of the concepts discussed around cooperative neutrality included a strong collaboration with military alliances and further partners, although the exact scope was not clearly specified. One form of increased collaboration could be the trade with weapons, weapon systems, and ammunition, which is (in 2023) still prohibited under Swiss law and could constitute a breach of relative neutrality obligations, depending on the circumstances: Switzerland could claim that it is trading with non-belligerent powers, who then further trade with belligerent powers—this would technically be within the scope of relative neutrality, although it could also be interpreted as a breach of relative neutrality obligations by a belligerent party. Furthermore, a strong collaboration with a specific military alliance and also specified further partners could also breach what is conventionally understood under the term “state neutrality” (see Definition 4.4.2).

As discussed, some intermediary conclusions for the legal perspective with respect to cyberspace have already been made—further elaborations on the legal situation with respect to cyberspace follow in the upcoming chapter. Furthermore, the findings outlined so far, in particular with respect to state neutrality theory, form an important foundation for the understanding of what challenges cyberspace poses to neutrality, or how neutrality is challenged in cyberspace. The findings with respect to *conventional* state neutrality are essential for any considerations with respect to cyberspace in the upcoming chapters and sections.

The findings on conventional neutrality theory provided in this chapter also indicate that neutrality is still a relevant concept. The discussions following the Ukraine conflict, but also the rejection of a very ambivalent definition of neutrality by means of cooperative neutrality show that neutrality as a principle for Swiss foreign policy is still highly relevant and a topic contentiously discussed. The findings on neutrality theory in this chapter have shown how Switzerland is still understood to be a neutral country, despite its voicing of concerns of participation in sanctions following the Russian invasion of Ukraine in 2022: Based on the lemmas and definitions formulated in this thesis, Switzerland, as a neutral country, has an interest in maintaining its neutral role within the existing structures of the international system of states. This means that Switzerland will back international law in general, since it is also international law that provides the foundation of relative neutrality. An invasion of a country which is a clear breach of neutrality may, therefore, be condemned without affecting the neutral status of the country doing so. Furthermore, Switzerland maintains its permanently neutral role also within the framework of international collaboration through the structure of the United Nations or other international organisations. This established structure has implicitly been threatened by an actor that violates the basic principles of the established structures. It may, therefore, be seen as a valid approach in an active implementation of neutrality if these actions are condemned: Neutral countries tend to be conservative with respect to international structures, since the permanently neutral status is based on norms and, therefore, always is reliant on the status quo of international collaboration or institution; a consensus for the function of the neutral is required.

All of the arguments provided above are based on the principles outlined in the extended neutrality taxonomy earlier in this chapter. The example of how the findings may be applied, in order to explain and understand how neutrality is implemented in 2022 highlights the relevance of the findings in this chapter. The findings in this

chapter on conventional neutrality may be considered a necessity for the more fundamental question raised by thesis as to how the cyberrevolution affects the concept of neutrality. Nevertheless, they provide highly relevant insights by themselves and are applicable for understanding contemporary neutrality practice.

Chapter 5

State Neutrality in Cyberspace

This chapter adds considerations on cyberspace to neutrality, based on the findings from previous chapters on conventional neutrality theory and the international law concept of neutrality. The “fil rouge” is provided by the research questions from Chapter 1.

Section 1.6 specifically listed five points that are covered in this chapter. They are distributed in the sections in this chapter as follows:

Section 5.1 provides a synthesis of findings for the legal perspective and discusses them with respect to considerations on cyberspace from Chapter 2 and the findings on neutrality theory from Chapter 4. It further takes the reflections from the previous section and considers what might be plausible outcomes and challenges for permanent neutrality with respect to cyberspace. The section applies analytical theory development for advancing understanding of what could determine the characteristics of neutrality in cyberspace. Additionally, Section 5.1 juxtaposes these findings with the interviews mentioned in Chapter 1.

Thereafter, Section 5.2 adds real-world examples that inform on connections of neutrality and cyberspace. The section discusses the contribution of these examples to understanding the impact of the cyberrevolution on neutrality. Some of these examples are simply events that point towards additional challenges that could be investigated—unfortunately, their thorough investigation, for example by means of a case study, lies beyond the scope of this thesis. This is mainly due to the lack of available data on these examples. There is an example, which is investigated in more detail and suggests a concept this thesis defines as “legal signalling”. This “mini case study” on some legal aspects specific to Switzerland and its cybersecurity operations provides an important pointer to a potentially de-escalating influence of neutral countries when confronted with operations in cyberspace.

There is one cybersecurity incident in Switzerland, which may be of significance to neutrality and which received greater attention from the public. It also provides sufficient available resources and documents that can be consulted for a case study. This example is covered separately in Section 5.3, including a discussion on the implications of the case.

Finally, Section 5.4 provides a synthesis from all the previous chapters and formulates some lemmas for neutrality in cyberspace.

5.1 Theoretical Implications for Neutrality and Cyberspace

This section discusses the implications of the findings from previous chapters for the central research question and the specific research question. It recalls the main findings from Chapter 3 and reflects on the meaning of these findings on the background of this thesis' definition of cyberspace. This is also done for Chapter 4. Thereafter, Subsection these findings are juxtaposed with the contents of the interviews conducted a part of this thesis (see Appendix F), before some conclusions are drawn.

5.1.1 International Law Implications and Challenges

The main findings of Chapter 3 included an extensive discussion of legal perspectives on neutrality based on The Hague Conventions of 1907 [54, 55], and the resulting understanding of both the relative neutrality implications for conventional warfare as well as for some cyberspace scenarios. Some literature, such as the Tallinn Manual, but also further academic literature addressing relative neutrality law with respect to cyberspace, have been discussed; the most plausible interpretation of relative neutrality law has been extrapolated. Notably, the scenarios in Figures 3.1 and 3.2 were outlined with their respective implications for neutrality practice and potential challenges.

The findings from Chapter 3 can be summarised in the following lemmas:

*Lemma 5.1.1. **Relative neutrality is applicable to cyberspace.*** This follows generally from the discussions in Chapter 3 and was also concluded by Von Heinegg in his work discussed in Subsection 3.3.1. It is also a statement found in the Tallinn Manual.

On the basis of Lemma 5.1.1 one may conclude that, since permanent neutrality is based on relative neutrality, it is also possible to apply permanent neutrality principles on the background of cyberspace. Understanding what this might mean more specifically is one of the aims of the current chapter.

Lemma 5.1.2. Publicly accessible network infrastructure, even if located in a neutral country, may be used for message passing by the belligerent powers, even for CNA and CNE operations. This follows from the thorough discussion of the respective articles in The Hague Conventions discussed in Chapter 3. The scholarly work largely agreed with this approach of accepting the routing of messages, even if of a malevolent nature, through neutral territory. This also aligns with what is technologically feasible; inspecting every packet routed through a neutral country for malevolent content sent by belligerents would prove to be very difficult from a computer science perspective.

Lemma 5.1.2 covers what belligerents may do within neutral territory; it relies on an analogy to communication systems in general, for which rules are formulated in The Hague Conventions, as was discussed in Chapter 3. The following lemma states what belligerents are not allowed to do within neutral territory and, consequentially, also the duties following from this for a neutral country.

Lemma 5.1.3. Computer systems located in a neutral country, or under the sovereignty of a neutral country, may not be used by the belligerents for any activity. This applies equally to the general use of systems by armed forces, even if not for belligerent acts (i.e. not for conducting CNEs and CNAs), as well as for the use of computer systems specifically for CNAs and CNEs by belligerents. This follows from the inviolability of neutral territory, as is discussed in the Tallinn Manual (specifically: Rule 151), by Alexander Spring, and further publications covered in Chapter 3

The next lemma addresses the protection a neutral country enjoys under international law, with respect to cyberspace:

Lemma 5.1.4. Computer systems and further infrastructure forming part of cyberspace, such as network infrastructure, may not be damaged or otherwise affected by belligerent activities, also not as a side effect of belligerent activities, when it is located within neutral territory. This also follows from the legal considerations from Chapter 3. It is specifically in line with the formulation of Rule 150 in the Tallinn Manual but not with the commentary associated with that rule. As outlined in the respective chapter, this thesis disagrees with

the commentary's statement that side effects of belligerent operations are tolerable: This would form a significant breach of the nature of conventional neutrality rights. This view is also upheld by further authors, such as by Alexander Spring in his 2014 monograph [12].

The plausibility of this thesis' approach towards Rule 150 of the Tallinn Manual has been underlined in the discussions and analyses in Chapter 3, which directly leads to the formulation of Lemma 5.1.4 above. Lemma 5.1.4 does *not* affect the passing of IP traffic, as outlined previously in Lemma 5.1.2, or the delivery of "cyber means", as outlined in Lemma 5.1.5. The problem of "cyber weapons" or other "cyber means" of use to a belligerent passing through a neutral country's network, is formulated in Lemma 5.1.5:

Lemma 5.1.5. "Cyber means" that may be of use to a belligerent may pass through a neutral country, both virtually (through IP routing of traffic) or also physically (e.g., in the form of hardware that is sent by mail services to a belligerent) as long as this is not done on behalf of the neutral government; the delivery is ensured either through a public operator or a private operator providing services to the general public and the origin of the "cyber means" must not be the neutral government. As outlined during the discussion of Rule 151 in Chapter 3, the Tallinn Manual holds a different view, which presumably did not consider Article 7 of Document V of The Hague Conventions. The consequence of Article 7 is that weapons and ammunition may pass through the territory of a neutral country, as long as it is not by means of troops or convoys of a belligerent or in the sense of official support by a neutral government for a belligerent. The neutral needs to ensure that both belligerents are treated equally: It may not forbid the passing of weapons and ammunition for one belligerent while allowing it for another.

The following lemma specifies the steps a neutral country may take to defend itself against a breach of its neutrality rights:

Lemma 5.1.6. A neutral country may undertake (offensive) CNO in order to restore its neutrality, whenever its neutrality rights have been breached, without this being considered a breach of its neutral status. The reasoning for this interpretation is provided in the discussion of Rule 152 of the Tallinn Manual and is also supported by the commentary on that rule in the Tallinn Manual. This is an important finding enabling the neutral to take effective action against any belligerent activities against the neutral without risking a loss of the neutral status.

As stated previously, the neutral country has a duty to uphold its neutrality under certain circumstances:

Lemma 5.1.7. **A neutral country may not knowingly allow a belligerent to exercise CNA or CNE from computer systems located within the neutral's territory or otherwise under its control; if the neutral fails to terminate the exercise of CNA or CNE from computer systems within its territory or under its sovereignty, a seriously affected belligerent may take adequate steps to terminate these CNE and CNA, as long as these steps are proportionate and the neutral has been given the opportunity to respond to and correct the situation by its own means.** This is a fusion of Rules 152 and 153. As outlined in the discussion in Chapter 3, this strengthens the idea of neutrality as it prevents abuse of using the neutrality label. Furthermore, the rule also demands a neutral power to possess a minimum capacity with respect to CND.

Considering the lemmas stated so far, relative neutrality, when implemented in cyberspace, seems to be comparably effective with respect to contributing to national security and international stability. However, there are some fundamental drawbacks to this, which have not yet been considered:

Lemma 5.1.8. **The classification of the equivalent of an “attack” in conventional (kinetic) warfare is unclear; the Tallinn Manual only classifies a “cyber operation” as “cyber attack”, which is reasonably expected “to cause injury or death to persons or damage or destruction to an object”.** This definition would yield many of the lemmas listed so far less relevant. The Tallinn Manual's definition of a “cyber attack” outlined here was presented in Chapter 3. The ambiguity with respect to “cyber attacks” is a large problem: It may mean that many of the deductions from neutrality law for cyberspace are only applicable in a very narrow set of cases and interpretations as to when that law might be applicable may vary significantly. Furthermore, it leaves the question open as to what a neutral country should do in cases that do not fall under this definition of a cyberattack, but that are perceived by the country as unfriendly acts against its infrastructure. An example of such an activity is discussed later on as the RUAG Hack case. CNAs and CNEs, as defined in Chapter 2, may not fall under the Tallinn Manual's definition but might be relevant incidents for countries nevertheless that deserve a government response.

This is not the only challenge when considering the practicability of applying the lemmas derived from conventional neutrality law:

Lemma 5.1.9. The difficulty of attributing CNOs introduces further challenges for the implementation of relative (and permanent) neutrality in cyberspace. Chapter 3 outlined that the commentary to Rule 151 in the Tallinn Manual lists this requirement. It is also plausible that this is the case: Otherwise, a country could declare relative neutrality, then wait for a random CNO (depending on the definition of what constitutes a “cyber attack”), for example by private hackers, to be conducted, and claim this as a pseudo-valid reason for engaging against one of the belligerents, while being protected under the law of relative neutrality, since the neutral was supposedly only responding to a (falsely attributed) breach of its neutrality.

Therefore, the country that declares relative neutrality now already faces two challenges with respect to cyberspace: First, it needs to determine, when to classify a CNO as a “cyber attack”. Second, it needs to be able to provide proof of attribution, which is difficult to do (see Chapter 2 on the cybersecurity dilemma).

A further challenge is introduced by the following, which is partially a consequence of Lemma 5.1.8:

*Lemma 5.1.10. Many CNO are conducted in an environment of *unpeace* (see Chapter 2), i.e., they constitute hostile activities below the threshold of war. It is difficult to draw a clear line between espionage operations and cyber attacks, even when distinguishing espionage operations to be CNE and “cyber attacks” to be CNA.* This also poses difficulties with respect to intelligence collaboration or technical collaboration between national CERTs (see Neuman’s scenario presented in Chapter 3). An example for such a hostile act, which was conducted against Switzerland, is provided later in the RUAG Hack case.

The above leads to an additional conclusion:

Lemma 5.1.11. The revolutionary character of cyberspace manifests itself in the practical reality of the applicability of relative neutrality law. While many rules may be deducted in theory, their practical value is limited, since the revolutionary character of cyberspace introduces a high level of vagueness and ambiguity.

Nevertheless, countries do remain neutral during conflicts between third parties and manage to maintain their neutrality despite the difficulties formulated for cyberspace. It is plausible that the “workaround” for relative neutrality is to consider most activities in cyberspace to be below the threshold of war and, therefore, to not be a challenge to neutrality law. However, this would mean that relative neutrality

provides little to no use with respect to cyberspace. Indeed, the literature discussed does not cover any real-world cases of the application of relative neutrality law: If relative neutrality should only apply to cases that fall under the very narrow definition of a “cyber attack” discussed further above, only a very limited amount of cases for application exists (e.g., Stuxnet in 2007) and the cases known to the author of this thesis did not involve countries that maintained a claim to relative neutrality.

The lemmas discussed so far all cover relative neutrality. As discussed in Chapter 4, permanent neutrality, however, requires considerations from permanently maintaining a neutral status, i.e., also in the absence of a direct conflict between countries.

5.1.2 Permanent Neutrality Implications

The previous subsection illustrated some challenges posed to relative neutrality on the background of cyberspace. While these challenges may be resolved, the plausible resolution simultaneously yields relative neutrality for implementation in cyberspace less relevant: it is limited to a very limited and specific case of sets that rarely occur.

Lemma 4.3.1 (see Chapter 4) states that permanent neutrality relies on the definition of relative neutrality. Considering Lemma 5.1.1, which states that relative neutrality is applicable in cyberspace, this leads to the following conclusion:

Lemma 5.1.12. Permanent neutrality is applicable with respect to cyberspace since relative neutrality is applicable to cyberspace..

While this may—in theory—be true, the practical value of the findings on relative neutrality for cyberspace are of limited value, i.e., the formal definition of relative neutrality is an interesting reflection for understanding the conceptual challenges cyberspace poses to neutrality. However, instrumentally, the considerations on relative neutrality in cyberspace are of limited use for understanding permanent neutrality practice on the background of the cyberrevolution.

Nevertheless, this does not imply that there are no findings of practical value for permanent neutrality per se. The commitment to neutrality in case of a third-party conflict, already before such a conflict could be anticipated, is only one of the principles of permanent neutrality. The constant state of unpeace in cyberspace does pose particular challenges for permanent neutrality. How can a permanently neutral country respond to cybersecurity incidents that are below the threshold of war? The previous subsection has exemplified that neutrality law does not protect from hostilities below the threshold of war in cyberspace. The cybersecurity dilemma,

with its formulation of the problem of ambiguity for CNO and the vague definitions of what a “cyber attack” may be under international law lead to the following lemma:

Lemma 5.1.13. The cybersecurity dilemma and the ambiguity of the definition of what constitutes a “cyber attack” under international law, as well as the state of unpeace in cyberspace, generate challenges as to how a permanently neutral country should respond to cybersecurity incidents:

On the one hand, a strict response seems in the national interest for reasons of deterrence (according to Buchanan’s cybersecurity dilemma); on the other hand this might yield the neutral country to become less impartial, to be drawn into minor disputes with various parties, and to lose the trust it maintains under conventional permanent neutrality.

The challenge stated above may indeed be considered significant with respect to the central research question: It seems that a response by a permanently neutral country to a cybersecurity incident should be minimal due to the peace-promoting nature of permanent neutrality. However, this could be contrary to the national security interests of the neutral country. Interestingly, Switzerland has found an elegant solution to this problem, as is outlined later in this chapter.

Chapter 4 also outlined that there are further aspects of permanent neutrality: Notably, good services and the contribution of the permanently neutral to a balance of power. It is also interesting to consider what this could mean with respect to cyberspace. For example, a neutral country could provide forensic analysis services for cyberattacks, similar to the laboratories that already exist in Switzerland for the analysis of nuclear, biological, and chemical substances. This has, in fact, already been suggested in a newspaper article in NZZ written by Maeder on 18th March 2019 [120]. However, this could result in the neutral country being targeted by state actors that might not want to become subject to an independent and neutral attribution. On the other hand, the neutral country can gain important insights from the analysis work.

The neutral country would presumably require a strong cyberdefence capability regardless of whether it hosts a forensic laboratory for cybersecurity incidents or not: The findings in the previous subsection stated that relative neutrality imposes the requirement for the neutral country to prevent and defend itself against a potential breach of relative neutrality from a belligerent. This implies that a permanently neutral country would presumably require a particularly advanced ability to do so.

Further potential manifestations of implementing permanent neutrality on the background of cyberspace— with respect to good services—could be the provision of a multilateral approach to the challenges that cyberspace poses to conventional

No.	Interview Date	Background Interviewee	Topic
1	2017/03/27	A Swiss Public Official	State Neutrality
2	2017/04/11	A Swiss Public Official	State Neutrality
3	2017/04/13	A Swiss Public Official	State Neutrality
4	2018/03/26	A Swiss Politician and IT Entrepreneur	State Neutrality
5	2021/12/09	A Swiss Retired Diplomat and NGO Affiliated	Platform Neutrality, State Neutrality
6	2021/12/19	A UK Cybersecurity Expert and NGO Affiliate	Platform Neutrality, State Neutrality
7	2021/12/23	A Swiss NGO Affiliate	Platform Neutrality, State Neutrality
8	2021/01/05	A German NGO and Think Tank Affiliate	Platform Neutrality, State Neutrality

Table 5.1: Interviews conducted as part of this thesis (anonymised). The interview numbers with relevant content for this thesis are marked green.

security concepts. Later in this section plausible indicators are discussed showing that this is indeed one of the manifestations of how permanent neutrality is affected by the cyberrevolution.

Recent examples that illuminate the plausibility of the statements above are provided later in Subsection 5.2.

5.1.3 Juxtaposition with Interviews

This subsection juxtaposes some of the challenges outlined previously (including their potential solutions) with contents of expert interviews that were conducted as part of the research for this thesis. The overview of interviews conducted, which was already presented in Chapter 1, is listed in Table 5.1 as an *aide-mémoire*. The interviews are used to reflect on points on neutrality and cyberspace in this thesis. They may also yield additional, new approaches for solutions to problems identified—or, on the other hand, suggest further challenges. The findings identified in this thesis so far are extrapolated with the contents of the interviews in the following. The full interview notes are listed in Appendix F. The most important content from the interviews is summarised and discussed thereafter. Since not all interviews yielded relevant content for this thesis, only those that did are discussed here. The respective numbers of the interviews discussed are marked green in Table 5.1. The interviewees are referred to with feminine pronouns regardless of their actual sex or gender.

Interview 1

Interviewee 1 rejects “hack backs” as an option for a neutral country’s response to CNE and CNA. Indeed, as discussed in Chapter 3, a hack back could be considered

a hostile act by a country and, therefore, would be a breach with the principle of abstaining from the use of force. However, in case of an attack classified as a “cyber attack” in the sense of the Tallinn Manual, self-defence—and, therefore, also a hack back—is a justified course of action. While the interviewee’s statement is very clear, it refers to the application of hack backs during times of peace—or rather, *unpeace*. A hack back in such a setting would provide the foundation for an escalation, which is against the tradition of neutrality practice, as identified in Chapter 4. This point made by the interviewee, therefore, supports the findings made so far in this thesis.

The interviewee also mentions that diplomatic events hosted in a neutral country might be a target for state actors. This is plausible, although it is questionable whether it is the neutral country’s task to also defend international organisations. Nevertheless, the point suggests that a neutral country should have a sufficient cyberdefence capability, since also the host country of international organisations might be targeted as a side-effect, when an attacker targets international organisations. Furthermore, while a neutral country might not be expected to defend international organisations it hosts, it might nevertheless require the ability to support these organisations when their defences fail—both by means of governmental capability and capacity and by providing a capable private sector cybersecurity ecosystem. This also suggests that the idea of armed neutrality is equally important in cyberspace as it is conventionally, in order for a neutral country to be able to fulfil its function as a host of international organisations.

This point is further supported by the interviewee’s statement that there is no significant difference in the intensity or frequency of CNA or CNE against a neutral country when compared to other countries. Yet, vast majority of the attacks are purely criminal with no identifiable state involvement or incentive. Neutrality does not result in a significant difference in terms of the number or intensity of cybersecurity attacks—this implies that in terms of frequency or intensity, neutrality does generally not offer a higher level of protection from cyberattacks, since most attacks are of a criminal nature. When targeted by government actors (or government-supported actors), however, neutrality may well be a distinguishing feature to reduce such attacks.

The interviewee also states that intelligence and technological collaboration is paramount with respect to national security considerations in cyberspace. Chapter 3 discussed the point of intelligence collaboration and that it is necessary and in-line with relative neutrality law, as long as certain limits are respected. Therefore, also this point is in-line with the findings of this thesis so far.

Interview 2

The interviewee identifies confidence-building measures, discussions on norms, rules and principles, as well as capacity building as major foreign policy goals of Switzerland with respect to cyberspace. This is a consequence of Switzerland's activities under conventional permanent neutrality. The point is also discussed later on in Section 5.2 as a consequence from conventional neutrality theory with respect to cyberspace. It is plausible that a neutral country, if, conventionally, it defines its neutral role as contributor of mediation and peace support for the international community, it should also do so with respect to cyberspace.

The interviewee acknowledges the problem of applying international law and, particularly, neutrality law to cyberspace—therefore supporting the motivation for this thesis. She also acknowledges that offensive capabilities are essential for Switzerland: As mentioned earlier, this supports our statement with respect to armed neutrality and extends this principle to cyberspace.

Interviewee 2 further states that the classification of a cybersecurity incident (e.g., as an attack) is ultimately a political decision of the government. This statement provides a major justification for not limiting the *neutrality in cyberspace* discussion to relative neutrality law: The political decision, by a government, in the sense of a response to a threat or attack, is ultimately where the principles and tradition of permanent neutrality applies. Permanent neutrality guides the government's response with respect to challenging decisions involving other states. Particularly when the basis of international law provides a thin or no definition of a justified response, the response of the government becomes a very delicate topic: The government has to decide, how to respond while following its tradition and status as a permanently neutral country.

Interview 3

The interviewee raises the problem that the Tallinn Manual provides a purely western perspective. She supports the idea that neutrality is an instrument for avoiding participation in wars and is subject to national security interests.

The first point supports some of the findings and reflections in Chapter 3: Some of the arguments in the Tallinn Manual were found to be contradicting or biased in terms of interests of western major powers. Hence, the interviewee's statement supports the approach in this thesis to critically reflect the contents of the Tallinn Manuals and, where justified by consulting international law and technological givens,

to discard certain points made in the Tallinn Manuals while providing a more founded alternative.

Her second point is congruent with findings in Chapter 4 and further strengthens the points made there on the basis of the permanent neutrality case study.

Interview 5

The interviewee suggests that a forensic cybersecurity laboratory with an international mandate could be hosted in Switzerland, which could contribute to reducing the attribution problem. This suggestion provides an interesting role a neutral country could take with respect to improving international cybersecurity means. It has already been discussed in the previous subsection: On the one hand, such a laboratory would further strengthen the role of providing good services to the international community and extend these services to cyberspace—therefore, providing an example of how neutrality can be implemented on the background of the cyberrevolution. On the other hand, the point also implicitly suggests that the principle of armed neutrality has to be extended to cyberspace, as already previously discussed. Hosting a forensic cybersecurity laboratory could potentially increase the attack surface of a neutral country, as does hosting international organisations—yielding an effective cyberdefence capability paramount.

Interview 7

The interviewee states that a neutral actor might be particularly important due to the aspect of deniability in cyberspace (i.e., for implementing a “judge” function). She further states that engaging in cyberespionage operations is problematic for a neutral state since espionage operations could be part of a greater operation—e.g., reconnaissance for conducting a CNA.

The first point is reasonable when considering the idea of establishing an internationally mandated cybersecurity forensics laboratory already discussed. It might also be possible to implement a judge function in case the neutral country is trusted by the respective parties. As has been outlined in Chapter 4, the idea of a judge function can only be implemented, when trust has been gained—i.e., it requires a passive past in order to allow for the active role a judge takes. It might, therefore, be difficult to take on such a role permanently for a neutral country, in particular when considering the international constellation following the invasion of Ukraine in 2022.

The second point supports the thorough discussion in this thesis on CNA and CNE activities with respect to neutral countries: Neutral countries may conduct

their own intelligence activities, also in cyberspace. However the delicacy of doing so has been discussed in this thesis on the background of the cybersecurity dilemma. As discussed later in Section 5.2, a concept introduced in this thesis called *legal signalling* addresses this problem while maintaining the freedom of a neutral country to engage in intelligence operations in cyberspace, when required.

Discussion of Interviewee's Contributions

Several challenges and findings brought up previously are supported by the interviews. The interview's most interesting contributions are first listed and then discussed in the following paragraphs.

1. The engagement in 'hack backs', or in cyberespionage (CNE) operations seems to be a point of discussion for a neutral country. The question might arise, whether neutrality is in the national interest with respect to cybersecurity. As discussed, CNE and even hack backs are possible under certain circumstances—thus neutrality does not provide a significant obstacle for national cybersecurity interests. An interesting solution to this tension between national security and neutrality in cyberspace is identified in this thesis under the term of *"legal signalling"*;
2. intelligence collaboration and technological collaboration are vital for a country. It remains open to which extent such collaboration is compatible with an integral approach to neutrality, as already discussed in Chapter 3. Nevertheless, there is no fundamental reason that would restrict a neutral country completely from conducting intelligence and technology collaboration. While technological collaboration would presumably also be possible under integral neutrality, it seems likely that intelligence collaboration would be more restricted while not posing a challenge under differential or active neutrality;
3. several interviews state potential for "good services", for example by means of diplomatic initiatives or a forensic centre for the analysis of cybersecurity incidents hosted by a neutral country. Simultaneously, this emphasises and extends the principle of neutrality being armed for cyberspace, since a country providing good services might also increase its attack surface by doing so;
4. the vast majority of cybersecurity incidents does not emerge from states and, therefore, neutrality does not have a significant impact on the overall frequency of cybersecurity incidents in Switzerland.

5. the interviewee's statements implicitly support the findings and reflections in this thesis, suggesting that they are legitimate and logically consistent.

The first, second, and fourth points stated above are particularly important: the statements from the interviews on the one hand imply that there is a significant challenge for a neutral country on the background of cyberspace to balance its national security concerns with the implicit requirements of permanent neutrality. On the other hand, the fourth point also shows that in the vast majority of cases, neutrality does not influence the everyday business of a neutral country. Nevertheless, there may be incidents that do emerge from state actors and could affect a neutral country; even if their occurrence is low in terms of numbers, their impact might nevertheless be high and so it is relevant to reflect on how a neutral country may respond to such a situation. The RUAG Hack case study later in this chapter discusses such a case; furthermore, the subsequent section introduces an example of what this thesis defines as “legal signalling”. Legal signalling is an additional option that a permanently neutral country has with respect to managing state-backed cybersecurity incidents and, simultaneously, legitimately engaging in intelligence activities in cyberspace while limiting the escalative tendency of such activities suggested by the cybersecurity dilemma.

The second point in the list above refers to the potential of good services and balance of power that a permanently neutral country could contribute on the background of the cyberrevolution—this illuminates potential activities that might contribute to international stability.

5.2 Examples of Activities related to Cyberspace

This section provides and reflects on some examples that indicate how permanent neutrality might be practised on the background of the cyberrevolution. It does not provide thorough case studies as these require sufficient amounts of available data for analysis and reflection. For the following examples only limited data is available. This thesis focuses on providing the case of the *RUAG Hack* as a thorough case study, as it provides for ample documentary evidence.

The examples in the following nevertheless provide valuable indicators for gaining an understanding of permanent neutrality in the cyber-era: As indicators, they support the arguments in this thesis.

As an example, this section documents CNO that were conducted most likely by a foreign state against infrastructure in Switzerland that belongs to the *International*

Committee of the Red Cross (ICRC), which is hosted in Geneva. This is an example of how a neutral country may become a target of state-backed CNO due to its permanently neutral role as a host country for international institutions—and potential implications this has for the host nation of international organisations to provide cyberdefence capabilities for the institutions affected.

As a further example, various diplomatic initiatives and engagements of Switzerland are presented, which aim at fostering a more stable cyberspace. Thus, this example indicates how permanent neutrality contributes to international stability also in the cyber-era.

Finally, the most substantial and interesting example in this section, which may be considered a “*mini case study*”, is discussed: The concept of “*legal signalling*” is defined by this thesis as a suitable tool for permanently neutral states in order to circumvent the escalative tendency formulated in the cybersecurity dilemma, which could limit the possibilities of permanently neutral states with respect to conducting CNA and CNE. The concept of legal signalling may be understood as an element of permanent neutrality in the cyber-era that contributes to international stability. It has a de-escalating effect.

5.2.1 Attacks on the Red Cross in 2022

In 2022, a major cybersecurity incident was reported by the *International Committee of the Red Cross* (ICRC) in Geneva. This example is documented by means of only two newspaper articles—the documentary evidence is, unfortunately, limited, as already discussed. Nevertheless, this example provides a valuable indicator for this thesis’ argument.

First, a newspaper article released in the major German newspaper *Sueddeutsche Zeitung* on 20th January 2022 reported a “*major cyberattack against the ICRC*” [121]. The article reports that the attackers obtained data concerning 515’000 people from over 60 national branches of the Red Cross and Red Crescent. The people are said to belong to “highly vulnerable groups”. The article further states the ICRC’s concern about the potential abuse or publication of the data. Furthermore, it is stated that the ICRC has not been able to obtain any further details about the attackers.

A second newspaper article was published around a month later, on 18th February 2022 in the Swiss newspaper *NZZ* [122]. The article reveals further details that were released by ICRC about the potential attackers. While a direct attribution to a state is omitted, the ICRC states that the attacks were conducted in a “*highly sophisticated*” manner and included the use of zero-day vulnerabilities (see Chapter 2).

As documented by the article, the ICRC further claimed that the attacks had been tailored specifically for use against the ICRC. These are strong indicators of an attack backed by a state. The article further outlines how this is unprecedented since the ICRC was so far considered beyond the scope of state conflict and its neutrality had generally been respected by all states. The article further outlines that one of the problems this incident points to is that of missing norms with respect to cyberspace; the article promotes that such norms should be further established, in order to protect international organisations, such as the ICRC.

The example provides for some interesting reflections: On the one hand, the ICRC is an organisation under the protection of Switzerland. It is located in Geneva exactly because of Switzerland's neutrality and is under the protection of Switzerland (as the depositary state of the Geneva Conventions), as well as the world community. The example raises the question of whether Switzerland, as a neutral and host country to many international organisations, bears responsibility for the protection from such attacks—or at least for their thorough investigation. It seems plausible that Switzerland, as host nation, has a responsibility to not only provide a working cybersecurity ecosystem for its population, organisations, and businesses but also for the international organisations, such as the ICRC, to which it is officially a host nation. This may particularly be considered true for the ICRC, since Switzerland bears an implicit responsibility as depositary state for many international legal agreements that provide the basis for the ICRC's operations.

On the other hand, the ICRC is an organisation considered as *neutral* in the sense that it does not support specific states and their interests but supports humans on the background of international humanitarian law. The example shows that a neutral status does not protect from attacks *per se*. The article from NZZ [122] states that, in fact, many international organisations are targetted by cyber-criminals, since those organisations often hold valuable (or: sensitive) data and also manage large funds. Furthermore, it is likely that in this specific case, the ICRC has been targetted by a state—therefore, this example also indicates that neutrality does not protect from state-backed attacks *per se*.

5.2.2 Engagements for International Norms

This subsection aims at outlining some examples of Switzerland's engagement with respect to diplomacy in cyberspace. First, also some statements from the interviews

discussed in Subsection 1.5.6 provide insights into Switzerland's activities in the domain of cyber-diplomacy. In Interview 2, three foreign policy goals were stated for Switzerland as a permanently neutral country:

1. Confidence-building measures for the prevention of conflicts;
2. discussions on norms, rules, and principles (which are not legally binding but establish expectations and lead to predictability);
3. capacity building.

These foreign policy goals indicate that Switzerland, as a permanently neutral country, contributes to international stability with respect to cyberspace.

Two further sources that support this suggestion. Both sources emerge from the Swiss department of foreign affairs, FDFA:

1. An article on the official website of FDFA, as accessed in 2021, introduces the UN's "*Eleven norms of responsible state behaviour in cyberspace*" [123], which Switzerland supports and promotes. The website outlines Switzerland's history in propelling international norms building: Switzerland participated twice in a *UN Group of Governmental Experts* (UN GGE) format and attempted to foster broad consensus building, in order to advance international norms in cyberspace. An essential asset of Switzerland that supported it in its activities was the trust it receives from many countries throughout different "blocks" of the world. Furthermore, the website outlines how Switzerland also participates in the UN's *Open-Ended Working Group* (OEWG), which it also chairs. Furthermore, the website says that Switzerland's mission is to support the UN to "*promote dialogue*" [123]. The latter may be interpreted as a classical role as a *mediator* on the international stage (see Chapter 4).
2. The second source is *Switzerland's position paper on the application of international law in cyberspace* [124], which is an Annex document to the *UN GGE 2019/2021* introduced under bullet (1). It shows how Switzerland attempts to signal to the international the relevance of upholding conventional values also in cyberspace.

The sources above provide an example of Switzerland's provision of *good services* in a role of a mediator and promoter of a value- and rule-based co-existence in cyberspace. These examples are indicators for the continued relevance of permanent

neutrality for international stability. Switzerland on the one hand provides *good services* with respect to norms building and, on the other hand, this may also be seen as a contribution to the balance of power, when Switzerland attempts to bring opposing groups of countries around one table, in order to find a common denominator, as Switzerland has done through the OEWG. This example is also further supported by the suggestions of Dahinden in 2021 [41] that Switzerland should engage in norms and confidence-building, as outlined in Chapter 2.

5.2.3 Example of “*Legal Signalling*”

The concept of “*legal signalling*” has been discovered by the author of this thesis by means of an analysis of the legal situation in Switzerland with respect to conducting cyberoperations. While analysing the legal situation in Switzerland, it is striking that the deployment of CNA and CNE is clearly regulated and tied to simple conditions that have to be met. Since these legal texts are publicly available, any state can digest their meaning and anticipate whether or not a cybersecurity activity emerging from Switzerland might be a CNE or CNA. In this sense, the law provides a clear guideline, also for a state potentially experiencing attacks from neutral Switzerland, as to why such activities are deployed. In that sense, the law has a *signalling* effect for other countries that improves the potential classification and anticipation of activities emerging from the neutral. This is what is referred to as “*legal signalling*” by this thesis and is an original contribution of this thesis to the academic field of cybersecurity. The concept of legal signalling may also be considered to have a deterrent effect: A country engaging in activities against neutral Switzerland also has clear indicators as to what a response to these activities might entail. The clearly signals that CNE and CNA can and will be deployed, given certain conditions, e.g., a threat to national security or critical national infrastructure, are met.

These findings have been published by the author of this thesis as part of a conference paper in 2021 [3], which is listed in Appendix B. The following contents are to a large extent derived from the text in that paper. In the following, an analysis of Swiss law and an interpretation of the implications for permanent neutrality in the cyber-era is provided. It should be noted that according to the definition of CNA and CNE in Chapter 2, CNEs are operations that are purely aimed at extracting data without generating any impact on the target system. This is solely contained in the definition of CNA, according to Chapter 2.

Switzerland restricts any measures of CNE and CNA to a strict regime of control under its intelligence and military law. Military or intelligence entities are the only

actors in Switzerland that are legally entitled to execute CNE and CNA operations and may do so only when certain conditions are met. *Article 100.1* of the Swiss Military Law [125] covers military security, i.e. the protection of the infrastructure of the Armed forces. *Lit. c*¹ states that the Armed forces may “*in the case of an attack against military network and information systems take the required measures*” and “[the armed forces] *may infiltrate computer systems and computer networks that have been used for such an attack, in order to disturb, prevent, or decelerate the access to information; these measures require, except during times of declared engagement in national defence, the approval of [the Swiss government,] the Federal Council*”. While this article permits the deployment of CNA and CNE operations, these activities require explicit governmental permission or are restricted to times of active engagement in defensive missions. They are further limited to the case of a direct response to a discovered CNE or CNA operation. Moreover, *Lit. e* implicitly allows the deployment of CNE operations:

“[The armed forces take] *preventive measures* [against espionage, sabotage, and illegal activities] *and obtain the necessary information if:*

1. *The armed forces are engaged in peace support or national defence missions;*
2. *The armed forces are engaged in internal support missions and the [CNE] measures are explicitly permitted”.*

This implicitly restricts the armed forces from using CNA in peacetime, while allowing the use of CNE only when certain conditions are met. Since Switzerland has constantly deployed armed forces in peace support missions over the last decades, CNE can be considered a standard practice within the armed forces. However, it is noteworthy that the deployment of CNA operations is restricted to times of declared engagement of the armed forces in national defence missions or requires explicit permission from the Swiss government.

The intelligence law of Switzerland has been revised in 2016 and was subsequently approved by means of a popular vote (Swiss Department of Defence, 2020). The intelligence law regulates and restricts the deployment of CNA and CNE operations by the intelligence service [126]. *Lit. d* of *Article 26.1* defines the requirement of explicit approval for “*the intrusion into computer systems and networks in order to:*

1. *collect information present in these systems or transmitted from those systems;*

¹Lit. in this context is an abbreviation for *littera* and refers to a sub-clause of the respective legal Article discussed.

2. *disturb, prevent, or decelerate the access to information in case these computer systems and computer networks are used for attacks on critical infrastructure*".

This applies equally to activities on networks and systems based in Switzerland as well as abroad. Furthermore, *Article 37* defines that if “*computer systems or computer networks abroad are used for attacks on critical national infrastructure, the Federal Council decides on the implementation of [CNA] measures [abroad]*”, and that the “*intelligence service may infiltrate computer systems and computer networks abroad in order to acquire information [...] about activities abroad [...] The head of DDPS, after consultation with the head of the FDFA and head of FDJP, decides on the implementation of [CNE] measures*”. Hence, any CNE or CNA operation carried out by the intelligence service abroad requires the explicit approval by a number of ministers or a majority of the government ministers, respectively. Additionally, CNA may only be conducted by the intelligence service in the case of attacks against critical national infrastructure. The sole two entities in Switzerland that are entitled to carry out both CNA and CNE operations are, therefore, generally restricted to CNE during times of peace. Only very specific circumstances, such as a declared case of national defence, a (cyber) attack against military information systems, or a (cyber) attack against critical national infrastructure, permit deployment of CNA operations and require additional approval on the ministerial level. It is noteworthy that the armed forces are restricted to cases of self-defence (i.e., to protect their own infrastructure). The intelligence service, on the other hand, may deploy CNA operations in order to protect critical infrastructure providers. This presumably minimises the risk of CNA operations being understood as a belligerent act; a deployment of CNA operations by the armed forces would suggest a belligerent character.

The armed forces may further only engage in CNE operations required for the support of peace missions. The intelligence service may engage in further CNE operations in order to acquire information in the national interest but requires ministerial approval for the deployment of any such operations. As stated by Spring in 2014 and previously discussed, Switzerland’s “*permanent neutrality is the rejection of war as an instrument of foreign policy*” [12]. Therefore, the engagement of Switzerland in CNA operations appears to be a purely reactive scenario to clearly specified cases aimed at harming the national interests of Switzerland. With regard to the cybersecurity dilemma, as outlined by Buchanan in 2017 [26], this clear signalling contributes to a state of stability and predictability; Switzerland is not known for measures of “active defence” or “preemptive measures” in the international community and is generally considered a state that strictly complies with its own laws. Therefore, countries do

not have to fear CNA operations emerging from any entities in Switzerland unless a clear case of a (cyber) attack against critical infrastructure has been discovered by the Swiss authorities.

While the regulations for the deployment of CNE operations are less restrictive, a country experiencing CNE operations from Switzerland does not have to anticipate these measures being of a potentially belligerent nature, unless the very clear criteria that can trigger a CNA response are met. This has a potential deterrent effect while contributing to stability and predictability by means of the careful restriction of CNAs to specific cases. The law, as analysed in 2022, seems to indicate that deployed CNE operations are primarily used for intelligence purposes. Engagement in intelligence activities, which are tolerated by the global community as necessary although undesirable, could bear the risk of being interpreted as reconnaissance in preparation for CNA operations. Due to the strict restriction of CNA operations to very specific cases, however, an entity experiencing CNE that could be used for reconnaissance does not have to interpret this CNE as a potentially threatening or belligerent act unless it decides to engage in CNA against Switzerland itself.

This form of legal signalling may be interpreted as an elegant implementation of a workaround by a permanently neutral country, in order to follow national security interests while still implementing a de-escalating approach towards CNOs. Legal signalling may be considered to contribute to both national security—since it clearly includes an easily deployable option for CNAs if needed—and to international stability—due to its continued endorsement of refraining from the use of force (in cyberspace) as a means of foreign policy. The latter may be understood as a contribution towards establishing the permanently neutral’s trustworthiness. Furthermore, the clear indication in law of under which CNE and CNA are deployed might also have a deterrent effect: An attacker knows what to expect as a consequence of activities. If a country implementing legal signalling has a sufficient cybersecurity capability, an attacker can be deterred due to the potentially negative consequences in the sense of a hack back.

5.3 The Case of the *RUAG Hack*

This section provides a case study, which illuminates the contemporary relevance of neutrality on the background of the research questions of this thesis. The object of study for this case study is as follows: In May 2016, a cybersecurity attack on the

Date	Event
September 2014	First appearance of traces in logs. No logs are available before this date.
December 2015	First indications from external organisations about RUAG machines being affected are reported.
Presumably before January 2016 (exact date undocumented)	The Federal Council is informed of a major incident presumably involving a semi-state actor.
21 st January 2016	GovCERT.ch opens a major incident to investigate the attack.
22 nd –31 st January 2016	Incident response reaches peak activity: A task force is established and available data such as logs and disks are forensically analysed.
25 th January 2016	The federal prosecution service opens a criminal investigation concerning industrial espionage.
1 st –29 th February 2016	Monitoring of the attacker’s activities by GovCERT.ch is fully set up.
1 st March–30 th April	Enhanced monitoring is set up.
3 rd and 4 th May 2016	A newspaper article is released online first (evening) and the following day in the printed newspaper by Tages-Anzeiger, which discloses the RUAG Hack to the public. This impacts the ongoing investigation, as the attackers are now aware that they have been discovered and that their activities are being monitored. The article claims the attack might have originated from Russia.
4 th May 2016	Almost simultaneously with the public disclosure, the Swiss Federal Council (government) releases a press statement [127], which outlines how the administration responded to the attack since its discovery.
23 rd May 2016	GovCERT.ch releases a technical report on its website [128], which explains the technical details around the RUAG Hack and the administration’s handling of the attack after its discovery. Furthermore, the Federal Council published 14 countermeasures implemented, in order to reduce the likelihood of data theft by the attackers.

Table 5.2: Timeline of the *RUAG Hack* case. Any events preceding the public disclosure of the case (3rd May 2016) are extracted from the RUAG report [6] (see Subsection 5.3.1) and the timeline therein on page 32.

Date	Title	Source	Ref.
2016-05-03	Cyberangriffe aus Moskau	Der Bund	[129]
2016-05-04	Geschäftsprüfungsdelegation wollte Geheimhaltung aufheben	NZZ	[130]
2016-05-04	Cyber-Attacke auf die Ruag: Bundesrat setzt Taskforce ein	Der Bund	[131]
2016-05-04	Ruag-Hackerangriff: «Es war Russland»	Handelszeitung	[132]
2016-05-04	Cyber-Spionage-Angriff auf RUAG	Federal Council press release	[127]
2016-05-04	Rüstungsfirma des Bundes gehackt	NZZ	[133]
2016-05-04	Cyber-Angriff auf die RUAG: begleitende Oberaufsicht durch die GPDel	Parliamentary Control Delegation press release	[134]
2016-05-06	Russische Hacker mit totalem Zugriff	Der Bund	[135]
2016-05-08	Geheime Schweizer Elitetruppe enttarnt	Der Bund	[136]
2016-05-08	Russische Hacker enttarnen geheime Schweizer Elitetruppe	NZZ	[137]
2016-05-12	Fall Ruag: Bund fürchtet das Schlimmste	Der Bund	[138]
2016-05-12	Ruag-Spionage: Outlook-Daten betroffen	Der Bund	[139]
2016-05-15	Bund war wohl das Ziel der Ruag-Hacker	Der Bund	[140]
2016-05-15	Hackerabwehr: Dem Geheimdienst sind die Hände gebunden	NZZ am Sonntag	[141]
2016-05-15	«Firmen müssen sich selbst vor Hackerangriffen schützen»	NZZ am Sonntag	[142]
2016-05-15	Ruag: Cyberattacke zielte auf VBS	NZZ am Sonntag	[143]
2016-05-18	Defence firm says no sensitive data acquired in hack	swissinfo.ch	[144]
2016-05-23	Ruag-Hacker haben 20 Gigabyte Daten entwendet	Der Bund	[145]
2016-05-23	Mehr als 20 Gigabyte Daten entwendet	NZZ	[146]
2016-05-23	Erkenntnisse im Zusammenhang mit Cyber-Spionage-Angriff auf RUAG	Federal Council press release	[147]

Table 5.3: Chronological listing (release date) of articles and publications from 2016 discussed in the RUAG Hack case study.

government-owned Swiss defence contractor *RUAG* was disclosed to the public. This thesis refers to it as the *RUAG Hack*.

The case study analyses a neutral state's response to a cybersecurity incident, which was presumably conducted by state-backed groups. The incident was below the threshold of war. Its analysis addresses the *ambivalence* stated in Conjecture 2. More specifically, the question of how neutrality policy is relevant both for the international community (in a "de-escalating" sense, contributing to international stability) and the neutral country implementing it (in terms of "signalling" and a contribution to national security) is illuminated by means of this case study.

This case study relies on methods for case study research, as outlined in Chapter 1. The attack covered by the case study is limited by the events as shown in Table 5.2, which are discussed in detail later in this section. The events occurred between September 2014 and May 2016. The media coverage, and therefore the documentary evidence investigated by the case study, covers media articles released in major Swiss newspapers from 3rd May 2016 throughout the remainder of that year. An overview of these articles is listed in Table 5.3. Some consequences of the attack are discussed on the basis of articles released in 2018 and 2019, which are listed in Table 5.4. Also, the case study considers official press releases of the government and parliamentary investigation reports released in 2016 and 2018 also listed in the respective tables, as well as a detailed technical report published by GovCERT.ch, the *Computer Emergency Response Team* (CERT, see Chapter 2) of the Swiss government, in 2016 [6].

The theoretical setting of the study relies on the theories and concepts of neutrality, as outlined so far in this thesis. The study reflects the RUAG Hack and the government's response, as well as the potential effect of the events outlined. The study juxtaposes Switzerland's response to the RUAG Hack to the implications of the *Cybersecurity Dilemma* (see Chapter 2). The resulting reflections illuminate the question of how neutrality can be beneficial for both the international community and the state implementing neutrality, i.e., Question 1 and Question 3. In a wider sense, the case enables us to understand how neutrality is still an up-to-date concept (see Question 2).

A major contribution of this case study to this thesis is the finding that a neutral country can indirectly attribute an attack to a country without an official government statement on an attribution. Through this, the neutral country avoids a "blame game" that often follows official government attribution statements—attribution is almost impossible to fully prove and a minimal level of plausible deniability by the country

Date	Title	Source	Ref.
2018-05-08	Cyberangriff auf Ruag – Lob und Tadel für das Verteidigungsdepartement	NZZ	[148]
2018-05-08	Cyberangriff auf die RUAG: Angemessene Massnahmen des Bundesrates und des VBS, aber ungenügende strategische Steuerung	Parliamentary Control Committee press release	[149]
2018-05-09	Die Ruag enthält dem Bund Informationen vor	Der Bund	[150]
2018-08-27	Bundesanwaltschaft sistiert Verfahren zu Cyberangriff auf Ruag	NZZ	[151]
2019-03-18	Der staatliche Rüstungskonzern Ruag soll grösstenteils privatisiert werden	NZZ	[152]

Table 5.4: Chronological listing (release date) of articles and publications from 2018 to 2019 discussed in the RUAG Hack case study.

accused is almost certain. Furthermore, the case study illuminates how a neutral country can deter by means of releasing detailed technical reports of cybersecurity attacks: The release of such reports deters in two ways. First, the ability to produce a detailed technical report of an attack reveals a sufficient cyberdefence capability of the respective country, which might render potential attackers cautious. Second, a publicly released technical report yields any deployed zero-days less effective; after the release of these reports the attack patterns will no longer be considered zero-days, since they are publicly known and any institution or country can implement protection measures against them. This is a high cost for an attacker, as a zero-day will be “destroyed” after it has been deployed against the neutral country.

The structure of the upcoming subsections is as follows: First, Subsection 5.3.1 discusses the detailed report released by GovCERT.ch in May 2016 [6]. Subsection 5.3.2 and the following discuss the public disclosure of the attack: The public disclosure of the RUAG Hack in Tages-Anzeiger is covered first, followed by the government’s press release and further public discussion, and the effect of the release of the RUAG APT Report on the public discussion. Finally, Subsection 5.3.8 summarises themes and formulates conclusions from the analysis and discussion of the RUAG hack.

5.3.1 Findings of the RUAG APT Report

On 23rd May 2016, the governmental cybersecurity entity of Switzerland *GovCERT.ch*, which is now part of the *National Cyber Security Centre* (NCSC), released a techni-

cal report about the RUAG Hack [6]. It is referred to in this thesis as *RUAG APT Report* or simply *RUAG Report*. The report documents the technical details of an attack that it claims has affected the systems of RUAG since at least September 2014 and provides a timeline of how the attacks went about². Relevant events from this timeline have been merged into Table 5.2, which shows an overview of all events deemed relevant for the RUAG case. The contents of the report and the timeline are summarised and discussed in the following.

The report states that the attacks might have started earlier than September 2014. However, the unavailability of older logs prevents data gathering for an analysis prior to this date. Nevertheless, it is noteworthy that one year and two months pass between the first data traces of the attack available (September 2014) and the first indication of an attack reaching the Swiss authorities (December 2015): The attackers had access to the network for at least that duration, potentially even longer. During that time they could infect further machines on the network and were able to exfiltrate data. An incident was only opened by GovCERT.ch in January 2016. Had the Swiss government not received indicators from other (foreign) organisations, the attackers might have been able to act undetected for an even longer period.

Hence, even as a neutral country, Switzerland relies on collaboration with other countries, in order to maintain an effective capability for combating cybersecurity threats. Common intelligence collaboration mechanisms for exchanging information are used by the Swiss government, as has already been outlined previously in Subsection 5.1.3 (see Interview 1). This includes technical and non-technical information and threat intelligence sharing groups in Europe. It is plausible that GovCERT.ch might have received information about the attack through these channels in December 2015. The report explicitly states that the discovery only occurred after receiving information from a foreign government entity. Therefore, external (governmental) organisations who were likely aware of the use of certain Command and Control (C&C) servers used by attackers probably saw that these servers were also contacted by IP addresses of the Swiss government-owned defence contractor RUAG. It is likely this discovery was their motivation to share this knowledge with Swiss government entities, such as GovCERT.ch.

The RUAG Report outlines further findings made by GovCERT.ch: First of all, it provides an analysis not only of the specific malware used for attacking RUAG, but also the greater context of the malware *family*, the malware's dependence, and its evolution from other similar malware.

²See page 2 of [6]

The malware identified in the RUAG case is called *Carbon-DLL* and *Tavdig*³. Nevertheless, the report also explains other related malware of the *Turla* family, also known as *Uroburos*⁴: The initial malware the family is based on is *Agent-BTZ*, which came up before 2007. Related mechanisms have been found in the *Carbon Rootkit* around 2007 and *Snake* around 2013. Snake is also classified as a descendant of Carbon Rootkit since it includes some enhancements to its code/mechanisms. It also includes some code/mechanisms found in Agent-BTZ, which is no longer present in the Carbon Rootkit. The report outlines how Carbon-DLL, which was the malware used for the RUAG Hack and found the first “in the wild” around 2012, is a further descendant of the Carbot Rootkit. The Carbon Rootkit bypasses certain safety mechanisms in specific versions of windows that have yielded the exploitations present in the initial Carbon Rootkit more difficult. Agent-BTZ, Carbon Rootkit, Snake, and Carbon-DLL are all used as what is referred to as *stage 2 malware*. This type of malware is used for data exfiltration after an initial reconnaissance phase. It is more complex than the malware used for an initial reconnaissance phase and is only deployed once the reconnaissance phase has identified machines and contents that might be of interest to an attacker. The reconnaissance malware used in the RUAG was identified as *Tavdig*⁵. According to the report, it is also occasionally referred to as *Wipbot* or *Epic* and was discovered for the first time around 2011. It is related to a reconnaissance malware named *Regbackup*, which occurred first around 2011.

It may seem strange that the report provides such a detailed, technical analysis, while not paying any particular attention to attributing the malware to a particular group of cyber-criminals or even a state. However, the detailed technical analysis in the report presumably pursued a set of very clear and plausible goals:

1. The publication of technical details might be understood to have a deterrent effect in the sense of a *show of force*: The very detailed technical analysis reveals a certain level of expertise of GovCERT.ch, which might deter a future attacker, since it may expect to be discovered;
2. the publication of a very detailed analysis also entails another deterrent component: The malware may be rendered useless for future use, or at least its set-up and protection measures against it will become part of generally available knowledge. This is particularly impactful for the attacker, in case the

³See page 15 of GovCERT.ch’s RUAG Report [6]

⁴See for example page 3 of GovCERT.ch’s RUAG Report [6]

⁵See page 15 of GovCERT.ch’s RUAG Report [6]

attack relied on a zero-day vulnerability, which now becomes revealed by the publication of the report. A future attacker will think twice before risking the potential revelation of a valuable zero-day.

3. the complexity of the attack, which is revealed by the detailed technical analysis, implicitly suggests that this attack was carried out by a state actor without explicitly stating so;
4. while the report does not explicitly state the origin of the malware and its descendance, the detailed listing of the different malware names that contributed to the specific malware used for the attack enables any member of the general public to search for publicly available attributions of the respective malware.⁶

The point outlined under bullet (2) is further backed up by the report: Its conclusion⁷ underlines the importance of sharing detailed malware information publicly, in order to enable partners as well as the general public to be aware of attack vectors, detection and prevention measures.

5.3.2 Public Disclosure of the RUAG Hack

The RUAG Hack was publicly disclosed on 3rd May 2016 by means of a news report in the Swiss newspaper *Tages-Anzeiger* [129].⁸ The article triggered a public discussion of the case, its implications, and its background; multiple newspaper articles listed later in this section evidence this discussion.

⁶For example, the following Wikipedia article will provide a means for further research on the background and origin of the *Turla* malware family to any interested member of the public: [https://en.wikipedia.org/wiki/Turla_\(malware\)](https://en.wikipedia.org/wiki/Turla_(malware))

⁷See page 29 of GovCERT.ch’s RUAG Report [6]

⁸The online version of the newspaper is accessible at <https://www.tagesanzeiger.ch/>. Tages-Anzeiger is part of *TX Group* (<https://tx.group/>), a public limited company owning multiple newspapers in Switzerland. Tages-Anzeiger shares its editorial office for national and international content with other media of the TX Group-owned *Tamedia* network (<https://www.tamedia.ch/>), all of which are owned by TX Group. Articles containing national or international news are usually available in all newspaper portals of the Tamedia network. For reasons of accessibility through subscription, the author of this thesis has accessed all articles that have been published in Tages-Anzeiger through the news portal of the Bern-based Swiss newspaper *Der Bund* (<https://www.derbund.ch/>). The references to the articles, therefore, point to the website of Der Bund and the articles are referenced as published in Der Bund, although they have also (and often first) been published in Tages-Anzeiger. This structural set-up of the shared editorial office and common publication of articles with national and international content on all websites of Tamedia newspapers is also evident from the imprint of Der Bund and Tages-Anzeiger at <https://www.derbund.ch/impressum-der-bund-239668062014> and <https://www.tagesanzeiger.ch/impressum-tages-anzeiger-876605432348>, respectively.

The initial article disclosing the RUAG Hack to the Swiss public formulates the assumption that the hack has been carried out by state-sponsored Russian hackers. Furthermore, the article probably relied on an internal source of the Swiss Department of Defence (DDPS), the Office of the Attorney General of Switzerland (OAG, the federal prosecution service⁹), or the Federal Assembly (Swiss Parliament), since these entities had received information about the RUAG Hack several months prior to its public disclosure. The article is clear about the hack and its supposed origin but it is vague in terms of stating the explosiveness of the disclosure: it explains an attack on RUAG happened, alongside a critical reflection on a report published by the Federal Intelligence Service (FIS) the same week [153], which mentions cyberespionage as a tool increasingly used for gaining access to confidential information by foreign services. The article seems to specifically avoid a scandalising or “red-top” tone: the information on an attack having been discovered by DDPS in January 2016 almost reads like a side-note to the comment on the FIS report; it might almost seem as if the fact a cybersecurity incident had occurred several months before was already known to the public and the article was rather criticising it was not mentioned in the FIS report.

Subsequently, the article continues to outline an attack on servers of RUAG had occurred and that this had led to greater amounts of data being leaked to the attackers—again, this is presented in a style that resembles a summary of already previously publicly disclosed cybersecurity incidents. The first time the article indicates it contains exclusive information is when it reveals that the information leaked during the attack on RUAG is—according to internal sources—of “*highly confidential*” nature and that it affects interfaces to DDPS and the Swiss Armed Forces. However, it is also stated that DDPS has already claimed that it has “*not identified any damage in its IT infrastructure*” resulting from the attack on RUAG. The article further reveals steps the Swiss Confederation had taken after discovering the incident while not disclosing it to the public:

- initially, the Federal Council had been informed;
- the federal prosecution service opened a criminal investigation as early as 25 January 2016 concerning industrial espionage;
- the Federal Council defined 14 countermeasures on 23rd May 2016, aimed at reducing the likelihood of data theft by the attackers.

⁹This thesis refers to OAG mostly as the federal prosecution service, in order to ease the understanding for British readers.

The criminal investigation of the case was aimed at industrial espionage, not state-level espionage or even an act of war—even though DDPS and the Swiss Armed Forces were allegedly affected by the RUAG Hack. The effects of the RUAG Hack on the Swiss Confederation are also evidenced by the 14 countermeasures defined by the government and the statement from an internal source of the Swiss administration that “highly confidential” data was affected.

The article further states that it is not the first cybersecurity incident against the Swiss administration and connects the RUAG Hack to a series of incidents that occurred between 2008 and 2012: those attacks had been traced back to a building in Moscow allegedly owned by the Russian state. The article further claims that the RUAG Hack, since it is probably connected to Russia, might further negatively impact the relations with Russia; these have been difficult since the invasion of Crimea in 2014 and Switzerland’s subsequent sanctioning of Russian oligarchs—Russia allegedly considers this a *breach of neutrality policy*.

The article concludes by explaining the difficulty of investigating cyberattacks of this kind and that the federal prosecution service has had to halt its previous investigations in such cases due to the lack of sufficient hard evidence, even though soft indicators seem to identify a potential source of the attack quite clearly. This indirect attribution is discussed in Subsection 5.3.1.

Even though the article does at some point mention it provides exclusive internal information, this is only mentioned in connection with the classification of government data that is assumed to be affected by the incident. As already mentioned, in the original article it seems the author deliberately avoids mentioning that the article is an exclusive disclosure of the case. Only in a follow-up article released later the same in the same newspaper it is specifically labelled as “*exclusive disclosure*” [131]. That follow-up article further states the Federal Council (Swiss government) had appointed a task force in order to define immediate measures against the attack and to further protect the infrastructure.

5.3.3 Immediate Publication of Further Details in the News

Following the disclosure of the RUAG Hack by means of the article discussed in the previous subsection, a number of newspaper articles followed that cited the original article and also disclosed further details. Some of these articles are listed in the following:

- As already mentioned, a follow-up article [131] (released by Tamedia on 4th May 2016) explicitly labels the original article as “exclusive disclosure” of the RUAG Hack. The further focus of that article is to refer to a government press release, which provides some background information on the government’s counter-measures after the government discovered the attack. The respective press release is thoroughly discussed in Subsection 5.3.4. The article further states that according to internal sources of the federal administration, the attackers have been traced to a building in Moscow that is attributed to the Russian state.
- An article released by Handelszeitung on 4th May 2016 [132] emphasises the Russian origin of the attack. It repeats some of the findings of the original disclosure and also emphasises an interview¹⁰ with the head of DDPS, Federal Councillor Guy Parmelin, who states that the DDPS had also been subject to a cyberattack in January, during the *World Economic Forum* (WEF). However, that attack was not connected to the RUAG Hack and it seems it might have been mentioned in order to explain that attacks against the federal administration are not uncommon. On the other hand, it should be noted that the RUAG Hack was fundamentally different in that it included an APT and was high complexity (as discussed in Subsection 5.3.1), as opposed to the WEF-related attacks. Those were based on Spam e-mails [154].¹¹ The Handelszeitung article further outlines how the parliamentary *Control Delegation*¹² (CDeI) pushed for the de-classification of the RUAG Hack from “secret” to “confidential”.

The problem with a classification of “secret” is that only a very limited number of personnel may access the information, while “confidential” allows broader access. The CDeI was concerned that effective counter-measures were not possible in case of a too high classification, while the government apparently classified the secrecy of the incident higher (see also Subsection 5.3.4 on details concerning a press release by the CDeI the same day). It is possible that

¹⁰The interview [154] was released by the Tamedia newspapers on 4th May 2016, together with the printed version of the original article (the web version of that article had been released on Tuesday, 3rd May 2016).

¹¹Spam e-mails have emerged as unethical and often also illegal methods of mass-marketing. The term generally refers to unwanted messages received by e-mail. Spam e-mails may be used for attacks if the aim is to retrieve users’ credentials, spread malware, etc. For a thorough overview of what the term “spam” refers to and how it may be used for attacks, see Finn Brunton’s 2013 book *Spam* [155]

¹²The Control Delegation is called “*Geschäftsprüfungsdelegation*” (GPDeI) in German and oversees the activities of state security and intelligence services or matters that must be kept secret, is outlined on the website of the Swiss Parliament, as accessed in 2022 [156].

the government’s position to maintain a classification of “secret” might have been due to indecisiveness in the government regarding how to best respond to the incident. The article further states that the president of the CDel, Alex Kuprecht, said: “*we know that it [the RUAG Hack] was Russia*”.

- Two further articles [130, 133] published the same day (4th May 2016) in NZZ¹³ (one online and the other in the printed version) reiterate most of the contents already covered in the discussion of the previous articles. The content of the two articles is very similar, although it is presented slightly differently in the online version as opposed to the printed version. The online version mentions that Federal Councillor Guy Parmelin (head of DDPS) said it was a case of industrial espionage, while the printed version states espionage in general. The printed version further connects the case to previous attacks on the federal administration: an attack on FDFA and the State Secretariat for Migration (SEM) in 2007, which emerged from African hackers, and attacks against FDFA in 2009 and 2012, where thousands of computers had to be disconnected from federal networks as a consequence. The article states the difficulty of finding the attackers in both cases. The articles also mention that DDPS / the Swiss administration was planning on disclosing information about the attack to the public regardless of the newspaper disclosure on the same day.

The articles published on 3rd and 4th May 2016 share a number of themes:

- They highlight the difficulty of cyberespionage incidents being investigated and prosecuted by the authorities;
- they show a tension between the parliamentary Control Delegation and the Federal Council in terms of classification of the case: the CDel was pushing for declassification in order for the incident to be dealt with properly within the administration while the government seems to have had an interest in keeping the number of people who know about the case as low as possible. This indicates that the government might have been indecisive in how to deal with a case;

¹³NZZ is often considered Switzerland’s most intellectual newspaper, i.e. articles and analyses are very founded and it is also read in other German-speaking countries and internationally, as is evident by its international edition. Furthermore, it was ranked as the best newspaper by a review in 2016 (the year of the RUAG Hack) [157]. The author of this thesis, therefore, considers it a very trustworthy source of information.

- the government labels the case as “industrial espionage” and emphasises it is an attack on a business (although RUAG is fully owned by the Swiss Confederation), while some of the articles emphasise that DDPS and other parts of the administration might have been affected by the attack due to the strong ties of the IT systems of the administration and RUAG;
- the articles imply that the government might have wanted to keep the case secret, even though the government claims it was planning on releasing information regardless of whether a public disclosure by the newspapers occurred or not;
- The government does not comment about the origin of the attack, while the newspapers clearly attribute the attack to Russia.

5.3.4 Government and Parliament Press Release

The Swiss government (Swiss Federal Council) published a press release [127] on 4th May, the day after the public disclosure of the RUAG Hack. This was most likely a response to the embarrassment of the public disclosure and in order to inform the public about the steps the federal administration had already taken before the public disclosure—however, the head of DDPS, Federal Councillor Guy Parmelin, claims a press release was planned either way (see Subsection 5.3.3). Also, the parliamentary Control Delegation published a press release on the same day [134]. In the following, the former is referred to as the “government press release”, and the latter is referred to as the “CDeL press release”.

The government press release states that the federal intelligence service had informed the federal prosecution service of a spyware infection at RUAG in January 2016. The federal prosecution service started a criminal investigation into potential industrial espionage on 25th January 2016. The press release further states what has already been outlined in Subsection 5.3.3: that the Federal Council defined 14 counter-measures on 23rd March 2016 and that, for historic reasons and because RUAG is an important business partner, the IT systems of RUAG and the federal administration are closely tied. The 14 countermeasures were focused on reducing the risk of data theft. Furthermore, a task force was defined, which should address the potential risk with respect to the close ties between the IT infrastructure of RUAG and DDPS; at the time of the press release, no damage to DDPS infrastructure could be identified. Additionally, the cyberattacks on FDFA (three cases within five years, see Subsection 5.3.3) and the assumed beginning of the RUAG Hack in December

2014 are mentioned. The report closes with a paragraph concerning RUAG and its countermeasures against the attack. The following formulation is noteworthy: *“The Confederation, in its role as owner of 100% of the shares of RUAG, takes note that, in connection with the incident, RUAG has initiated and implemented various immediate measures.”* The government press release, by using this formulation, creates a sense of distance and distinction between the government and its administration on the one hand and the company where the cybersecurity incident occurred on the other side. While the company is fully owned by the Swiss Confederation, the press release still implies it is an actor of its own, since the government merely “took note” of the actions taken at RUAG. This is noteworthy with respect to the classification of the case as industrial espionage (even though the main target of the attack might have been defence-related information obtained in RUAG): the government’s aim seems to have been to attempt, at this early stage, to not classify the attack as an attack against the Swiss Confederation or any of its entities but rather to portray it as an attack against a business. This is noteworthy for theoretical reflections in later subsections.

The CDel press release is similar in terms of content to the government press release: It states that the CDel had been informed of the incident towards the end of January and that, since it considered the case to be of a very serious nature, it had been conducting multiple investigatory questionings of different administrative authorities as well as with senior executives of RUAG from 22nd February onward. In this sense, the press release aims to assure the public that the situation had been taken care of adequately by the CDel, similar to the government press release, which also aims to assure the public that the situation had been handled appropriately by the government and the respective administrative authorities. The CDel press release further lists a series of events, which are summarised in the following (all dates refer to 2016):

- 22nd February: The CDel questioned the head of DDPS (Federal Councillor Guy Parmelin) on the risks of the attack for RUAG and the IT systems of DDPS. It discussed necessary mitigation steps. It further heard the federal prosecutor, who informed them about his steps in the ongoing criminal investigation.
- 23rd February: The CDel urged the Federal Council to undertake any necessary steps for mitigation, such that the public could be informed as soon as possible.
- 3rd March: The CDel discussed the current state of works with respect to the RUAG Hack and the next steps, after analysing a report written by the security

core group (consisting of the heads of FIS, the State Secretariat, and the Federal Office of Police, *fedpol*) for the Federal Council Security Committee (FCSC, consisting of the heads of DDPS, FDJP¹⁴, and EAER¹⁵).

- 14th March: The CDel led discussions with members of the FCSC, in particular concerning de-classification of the incident, as the CDel was concerned that the classification of “secret” would hinder an adequate response to the incident. FCSC, on the other hand, was convinced that the classification was necessary in order to take adequate countermeasures.
- 23rd March: The Federal Council made a secret decision on several measures, in order to respond to the incident.
- 13th April: The CDel discussed the secret decision on countermeasures of the Federal Council taken on 23rd March and conducted further investigative questioning of administrative entities¹⁶.
- 14th April: The CDel informed the Federal Council of its conclusions and raised its concerns with respect to the classification of the incident once again—the CDel expressed more clearly that its view was the secret classification of the incident posed a serious obstacle to a systematic response to the incident.
- 22nd April: The CDel held discussions directly with RUAG concerning the damage caused by the incident and asked which countermeasures along which strategic lines were decided for mitigation.

The CDel press release concludes by stating that the CDel will inform the parliamentary Control Committees (CC) in detail about its activities with respect to the RUAG Hack and that it will pursue further activities within its remit; however, it will not provide any further information about the incident to the general public, since this is within the remit of RUAG and the Federal Council.

The two press releases yield the following themes noteworthy for highlighting:

- The Federal Council (government) classified the event as “secret”, while the CDel pushed for a de-classification (according to articles discussed in Subsection 5.3.3, a de-classification to “confidential”);

¹⁴The Federal Department of Justice and Police.

¹⁵The Federal Department of Economic Affairs, Education, and Research.

¹⁶Namely these were the Federal IT Steering Unit (FITSU) and the Armed Forces Command Support Organisation (AFCSO).

- The government press release emphasises a distinction between the attack on RUAG—a government-owned private company—and the possible impacts of the attack on the federal administration. It is noteworthy that the government’s formulation emphasises that RUAG was attacked as a private company and that the government is not directly responsible for the action taken at RUAG and, therefore, the government avoids the RUAG hack to be considered an attack against governmental infrastructure, even though RUAG is fully owned as a private company by the Swiss Confederation. On the other hand, the government insisted the case should be classified as “secret” (as opposed to the option of classifying it as “confidential”), which seems slightly contradicting to the attempt to classify the attacks as a case of purely industrial interest in the activities of RUAG by the attacker. On the other hand, the government press release did admit that federal IT infrastructure might be affected due to historic ties between RUAG and federal systems and that respective investigations were ongoing;
- the press releases do not state the exact reason why there were different views on the classification. Apart from the technical reasons (*“honeypot”*) there might have also been political reasons, such as the need to respond to attempts of exfiltrating federal data and the connected public reaction;
- neither of the press releases states anything about the origin or complexity of the attack—it is noteworthy that the newspapers disclosing the RUAG Hack strongly focused on these aspects, while the press releases, being official and political documents of the Swiss Confederation, avoid any kind of attribution.

5.3.5 Further public discussion of the case in May 2016

Following the first articles disclosing information about the RUAG Hack and the official press releases on and shortly after 3rd May, the following days and weeks gave way to the disclosure of further information and discussion in the news. This subsection lists the most significant articles and other publications deemed relevant for the case (all dates in 2016):

- 6th May 2016: Tamedia newspapers release an article [135] stating that Russian hackers had complete access to RUAG’s servers and that potentially any digital data at RUAG might have been subject to data theft. This information is provided by two anonymous. The article states that according to undisclosed

sources within RUAG, cybersecurity attacks at RUAG are frequent and usually repelled but that the RUAG Hack was different in that it was conducted in a highly professional manner (implying a state-backed actor). The word “espionage activity” is used. The article also outlined that IT security experts working for the federal administration have uncovered striking parallels with attacks conducted earlier against the Swiss administration and that it is likely that the attackers operated from Russia. The article summarises the different attacks against FDFA in 2007, 2009, and 2012 and explains the indicators pointing towards a Russian origin.

- 8th May 2016: Tamedia newspapers further uncover the direct connection between the RUAG Hack and data potentially stolen from the Swiss Confederation [136]. The article released by Tamedia references an article in *SonntagsZeitung* [158]¹⁷, which claims that RUAG had been in possession of 30’000 personnel records of members of the federal administration and parliament. The newspaper explains that the data might have been accessed by the attackers as a consequence of the RUAG Hack. The article further references an article published in NZZ the same day [137], which suggests that the RUAG Hack attackers exfiltrated the personal data of the *Army Reconnaissance Detachment 10* (AAD 10)¹⁸, which is kept secret due to the delicacy of the detachment’s missions. This information is provided based on “*well-informed sources in DDPS*” [137]. Apparently, it was being discussed to provide a new identity for members of AAD 10. The content of the articles was also taken up the same day by the international (i.e., English-speaking) Internet news outlet of the Swiss Broadcasting Company on swissinfo.ch [159]. Although the articles do not elaborate on this, it is evident that the data of the AAD 10 forms only a small part of the 30’000 records of personal data potentially affected—which underlines the potential significance of the RUAG Hack for Switzerland’s national security.
- 12th May 2016: Tamedia newspapers release an article [138], which summarises the general story of the RUAG Hack and also addresses the problem of the potential data leak of sensitive data. Additionally to AAD 10, also personnel of the Federal Intelligence Service, FIS, is reported to be affected by the risks of

¹⁷The article in *SonntagsZeitung* is not further discussed, since the author had no direct access to it due to paywall restrictions. The article seems to be very similar in terms of content to the NZZ article from 8th May 2016 [137] discussed later on.

¹⁸See the following link for further details: <https://www.vtg.admin.ch/de/organisation/kdo-op/ksk/a-aufkl-det-10.html>

potential data theft. The article outlines that the data was provided for RUAG by the *Federal Office of Information Technology, Systems, and Telecommunication* (FOITT) in June 2015, in order to provide it for RUAG’s digital address book of federal employees. However, FOITT is cited in the article as having claimed none of the provided data was classified. It is not further elaborated upon whether this means the data might still be sensitive and contain data of AAD 10 or FIS employees but it is stated that the situation still seems to be unclear. The article also cites DDPS in saying that no employees of FIS are momentarily at risk. Additionally, the general problem of a number of businesses, which are strongly interconnected with the federal IT infrastructure, and the risk involved are discussed. On the same day, a further article was released by Tamedia newspapers [139], which provides more details on the data affected: It discusses the DDPS-internal communication about the RUAG Hack, which had only just been sent by email to its employees. The communiqué states that the directory data, which had been shared with RUAG, did not contain any private personal data. On the other hand, the article also states that it could not yet be ruled out that systems of DDPS might have also been affected by the RUAG Hack—in particular, systems and networks that are authorised to handle data classified as *confidential* and *internal*.

- 15th May 2016: A further article is published in Tamedia newspapers [140], which claims the Swiss Confederation presumably was the main target of the RUAG Hack. It references three articles published in *NZZ am Sonntag* on the same day. The first article [141] summarises an interview with the head of FIS, Markus Seiler, and highlights his point that Switzerland does not conduct counter-attacks in cyberspace (“hack backs”) in its regular intelligence operations, as the law does not generally allow this. Furthermore, this article states that it is meanwhile considered “almost certain” that secret data of the Swiss Armed Forces was obtained by Russian attackers—however, this is not attributed as a statement to Markus Seiler. The second article published in *NZZ am Sonntag* on that day [142] contains the actual interview with Markus Seiler. Noteworthy are his already mentioned highlighting of the missing possibility of “hack backs” for observing an attacker, in case of indicators for an attack exist. Furthermore, Seiler states that states’ operations (i.e., attacks) in cyberspace are mostly aimed against state administrations or state agencies, highly professional in terms of their implementation and very difficult to detect.

When asked whether this was also the case for the RUAG Hack, Seiler does not comment since the case is classified. The third article released that day in *NZZ am Sonntag* [143] provides insightful reflections and statements with respect to the RUAG Hack. First, it cites a spokesman of RUAG, who claims the attack was clearly aimed against DDPS. A press communiqué released by RUAG on 12th May 2016 [160] is referenced, which identified the DDPS as the only target but also stated that the malware was not transferred to any systems of DDPS. The article also states that the DDPS disagrees with RUAG’s formulation of being the main target and that DDPS emphasises that it was RUAG, not DDPS, which had been attacked. It is further addressed what diplomatic consequences the attack might have—FDFA says that it does not take any steps since the criminal investigation has not yet identified an attacker. However, a spokesperson of FDFA also clearly states that regardless of where the attack originated, this was an “unfriendly act” and that “friends do not treat one another like this”. The Russian embassy is cited as claiming that it does not express itself with respect to rumours. The article concludes that it is still unclear what data is affected and that there are differing accounts on the sensitivity of the stolen data and possible inferences possible from the directory data, even if it is unclassified.

- 18th May 2016: An article is published on [swissinfo.ch](http://www.swissinfo.ch) [144], which implies that the data of AAD 10 was not affected by the attack. It quotes RUAG, which has stated that no such data was affected. Furthermore, it quotes Alex Kuprecht, head of CDel, in saying that “*multiple gigabytes of data had been accessed in the hack*” [144] and juxtaposes this with RUAG claiming that only a very small part of its database had been hacked.

In the articles listed and summarised above, the following findings are noteworthy:

First, the articles continue to attribute the attacks to Russia (as a location) and to a state actor. Often the articles directly imply the Russian state as an actor. While the first articles still slightly elaborate on why this is the case and also imply that previous, very similar attacks (against FDFA) had been conducted by Russian state actors, this attribution is never contested and, eventually, fades into the background as the attribution to Russia seems to be a clear case. Nevertheless, none of the articles ever reference an official statement from Swiss state representatives that would attribute the attack to the Russian state. Some of the articles in Subsection 5.3.4

quote an MP saying that the attacks probably emerged from Russia—most articles reference their own anonymous sources from within DDPS.

Second, the articles focus on identifying the impact and main aim of the RUAG Hack. It is interesting to see that while federal government representatives focus on explaining that it was RUAG who was attacked and not DDPS, statements from anonymous sources in the federal administration as well as officials from RUAG seem to confirm that the main target of the attack was DDPS, even though the attack did occur against systems at RUAG. The articles and also government representatives, officials from RUAG and anonymous sources do not seem to agree and even contradict one another on the impact of the RUAG Hack on potentially sensitive data. They differ in the amount of data (small amount versus gigabytes of data) and also their sensitivity (unclassified data versus unclassified but potentially allowing sensitive data to be extracted versus confidential or even secret data). However, it seems clear that only data of DDPS was affected and, therefore, it is likely that the main target of the attack was indeed DDPS. This finding yields the question of why the federal government avoided acknowledging that DDPS had been the main target of the attack, why DDPS opposed a de-classification and also why it never officially attributed the attacks. These questions shall be addressed in Subsection 5.3.8.

5.3.6 Media Coverage Following the Release of the RUAG APT Report

The previous subsection covered the public disclosure of the RUAG Hack and any information revealed subsequently. The current subsection treats the publication of a technical report of the attack, which followed on 23rd May 2016. It focuses on the publication of the technical report as an event, rather than on its content, and on any newspaper articles surrounding it. The contents of the report are presented in detail in Subsection 5.3.1 and the impact of the report’s publication as well as a theoretical reflection are discussed in Subsection 5.3.8.

As outlined previously, the technical report, which in this thesis is labelled *RUAG APT Report*, was released on 23rd May 2016 by the government cybersecurity entity *GovCERT.ch*. Its publication was accompanied by a government press release on the same day [147]. It states that 20 gigabytes of data were stolen by means of the RUAG Hack and also asserts the attack had been conducted in a very targeted and professional manner. It further outlines that it is highly likely the data affected was

a directory serving as a source for Microsoft Outlook’s¹⁹ address book feature within the federal administration. However, contradicting “speculations” that had previously been spread, the press release clarifies that no private personal data of employees had been exposed. It further outlines that a technical report has been released with the goal to enable any other actors to detect and prevent infection with the malware. Furthermore, any attribution is explicitly omitted by the Federal Council due to the ongoing criminal investigation by the federal prosecution service. It should be noted at this point that the criminal investigation was later called off.

Two noteworthy newspaper articles were published the same day (23rd May 2016), one in Tamedia newspapers [145] and the other one in NZZ [146].

The Tamedia article [145] presents the information from the press release. It further includes a comment from the head of MELANI²⁰ (now part of Switzerland’s *National Cyber Security Centre* or NCSC), who outlines that it is most likely that the RUAG Hack was a case of industrial espionage since the attack revealed to the attackers which projects and activities RUAG was conducting. It further summarises some of the content from the RUAG APT Report and previous government press releases.

The NZZ article [146] is similar to the Tamedia article in terms of content. It elaborates slightly more on the aims of the attackers: Renato Kalbrmatten, the spokesperson of DDPS, is quoted as saying that a reconstruction of which data specifically might have been stolen is difficult but that it is certain that the highest security level of FIS employees has definitely not been affected since information about these employees is not included in the affected directory data. The article further quotes the head of MELANI that the attackers abruptly stopped any activities after the public disclosure of the attack at the beginning of May 2016.

It is noteworthy that both articles were designed in a way that seems in line with the press release of the government; no spectacular additions were disclosed and not even the attribution to Russia was repeated, which had been mentioned in earlier articles.

5.3.7 Later Publications

In the aftermath of the RUAG APT Report, the RUAG Hack was a less prominent topic but still occasionally appeared on the news or in publicly accessible reports.

¹⁹Microsoft Outlook is a common office computer application, which includes an email, calendar, and address book functionality. See the product webpage for further details: <https://www.microsoft.com/en-gb/microsoft-365/outlook/outlook-for-business>

²⁰MELANI was an abbreviation for *Melde- und Analysestelle Informationssicherheit*.

This subsection lists some of them for the sake of completeness, although most of the information does not provide any further insights for this case study.

First, a parliamentary question to the government [161] answered on 10th June 2016 uses the RUAG Hack in order to scrutinise the cybersecurity activities of the government. However, it does not provide any particular insights with respect to permanent neutrality, since it purely focuses on the scrutiny of administrative structures concerned with cybersecurity. A second parliamentary question [162], submitted by a different politician and answered the same day, has a similar focus. These activities in the parliament might, however, indicate efforts within Switzerland to increase the government's cybersecurity capability and capacity, which would be an indicator for the legitimacy of this thesis claim about the necessity of building effective cybersecurity capacities and capabilities in the sense of *armed neutrality*.

Second, on 8th May 2018, the Control Committee of the National Council (CC-N) published a press release [149], which gives a résumé of the case from the parliament's perspective. It references a detailed report about the case published by the parliamentary Control Committee²¹ (CC) the same day [163]. The content of the press release and the report are of operational character; they mainly explain that the government responded correctly but also demand consequences with respect to a dissolution of the IT infrastructure of RUAG and the federal administration, in particular their IT networks. It also reflects on how the experience of the RUAG Hack could influence Switzerland's cybersecurity strategy; however, this does not affect in any way Switzerland's neutrality policy or foreign policy/response to such an incident with respect to state involvement. Rather, it addresses the internal organisation of Switzerland with respect to responding to such cases. The report also demands that in the future important decisions with respect to such a case need to be documented, since this had not been done for the secret decisions made during the first stage of the RUAG Hack.

Third, the press release of 8th May 2018 was accompanied by two newspaper articles, one in NZZ later the same day [148] and another in Tamedia newspapers on 9th May 2018 [150]. Both articles reference the parliamentary press release and the associated report published on 8th May 2018. The NZZ article provides some interesting additional details: It states that the CC received detailed information with respect to the directory data affected by the RUAG Hack and that it subsequently deemed the RUAG Hack a "*very serious*" (literally: "*grave*") incident [148]. According to NZZ, the CC further criticised that DDPS did not sufficiently fulfil its scrutinising

²¹The Control Committee of both parliamentary chambers.

role as representative of the owner of RUAG, in particular with respect to the incident management of the RUAG Hack. The Tamedia article is very similar in contents; it also addresses the question of attribution and quotes Mrs Ida Glanzmann, a member of the National Council (federal parliament) and its CC, who claims that the CC did not receive any further information with respect to a possible attribution. The article mentions previous claims about Russia.

Fourth, an article in NZZ from 27th August 2018 [151] describes the federal prosecution service’s decision to close the criminal investigation concerning industrial espionage, which was initiated as a consequence of discovering the RUAG Hack. Apparently, this course of action was necessary since it had no hard proof in order to identify any delinquents. The article recalls the unofficial attributions to the Russian state and states that nobody is willing to confirm this attribution “*officially*” [151]. It does quote a spokesperson of the federal prosecution service, though, who says that “*in general*” [151] such complex attacks as in the case of the RUAG Hack could only be undertaken by state actors. The article also explains Switzerland’s general policy of not asking countries for legal assistance in cases where it is clear that the state itself was involved in a political offence, such as espionage. Again, the spokesperson is quoted that legal assistance only makes sense when the assisting state also has an interest in a criminal investigation.

Finally, an article published in NZZ on 18th March 2019 [152] announces the split of RUAG into two companies as a consequence of the problems identified in the aftermath of the RUAG Hack. A Switzerland-focused part of RUAG should mainly provide goods and services to the Swiss Armed Forces, while an internationally-focused company will continue to supply goods and services to third parties. This was presumably done in order to address the strong historic connection between RUAG and the federal administration, which had led to a strong interweavement of the respective IT systems.

The most noteworthy information of these last articles and publications may presumably be drawn from the information provided on and shortly after 8th May 2018 (the parliamentary CC report and subsequent the press release and articles), which classify the attack as very serious and elaborate on the complexity of attribution and the general practice of the Swiss Confederation with respect to espionage.

5.3.8 Analysis and Discussion of the Case

This subsection provides an analysis and discussion of the case described in the previous subsections. Some aspects of the case have already been outlined by the author

of this thesis in a conference publication in 2021 [3] (see Appendix B).

The case of RUAG Hack revealed an interesting approach to resolving some of the challenges for permanent neutrality outlined previously in this thesis: Following the discovery of the attack in 2016, the Swiss government’s computer emergency response team GovCERT.ch released a report (see Subsection 5.3.1). As outlined, the report provides a detailed analysis of the malware deployed. While the report does not explicitly attribute the attack to a state or a hacker group that might be affiliated with a state, it implicitly provides a plausible connection to the origin of the attack. Subsection 5.3.1 illustrated how the publication is an elegant instrument for deterring future attacks and “punishing” the attacker (by means of revealing zero-days used) while circumventing an attribution. An official attribution would be, as outlined previously in this chapter, problematic with respect to permanent neutrality principles. The attribution problem renders virtually all attributions acts of political opinion rather than acts of proof. As such, a permanently neutral country would find itself actively accusing another country without proper proof, which would yield an unseen precedent for permanent neutrality.

Themes identified from the reflections and discussions in this section are summarised in the following:

- The reliance of the Swiss government on foreign intelligence indicates a necessity for collaboration with other governments and services for threat intelligence purposes. This might seem problematic with respect to findings in Chapter 3 and, specifically, the discussion of a case raised by Neuman, in that the RUAG Hack was only discovered after the Swiss intelligence service received indicators from a foreign partner. However, the exchange of information happened on the background of regular intelligence collaboration and without the context of an open conflict between countries, in which neutrality law would apply. It seems that the exchange of information with respect to activities in cyberspace is a reality of the cyber-era required by national security interests. Such collaboration is not strictly a breach of relative neutrality obligations with respect to cyberspace. However, it could be seen as problematic with respect to an integral implementation of permanent neutrality in case the international environment changes, specifically on the background of a potential conflict—in that case a careful evaluation is required whether such collaboration is compatible with permanent neutrality and neutrality concerns have to be balanced with national security concerns. Since Switzerland implements an active approach towards permanent neutrality, this fact can be understood as an indicator that

active neutrality includes a certain level of technical intelligence collaboration with respect to cyberspace;

- the impact of the publication of the RUAG Report by GovCERT.ch have been discussed in Subsection 5.3.1. It includes a potential deterrence (also referred to as “signalling”) factor as well as a theme of indirect attribution (since the presumable attacker is not stated explicitly), which is further supported by the observation of the discussion in the media: Government entities never revealed where the attack originated from. Nevertheless, the newspapers very clearly point towards Russia, since the information publicly available virtually only allows this assumption. Furthermore, it seems plausible that government or parliament entities might have even leaked information on the origin of the attack in order to effectuate such an *indirect attribution*;
- A further theme, which might be considered mundane but nevertheless relevant, is that neutrality *per se* does not protect from state-backed attacks. This theme has already appeared in Subsection 5.2.1 with respect to the attacks on the ICRC. A neutral entity requires the ability to defend itself and neutrality *per se* does not protect from cyberattacks;
- a further finding from the media coverage is that the RUAG Hack seems to integrate itself into a history of similar incidents that even involved direct attacks on government infrastructure (e.g., on FDFA). Furthermore, the author would not know of any cases of a similar magnitude that emerged after the RUAG Hack. While it remains subject to speculation whether this was a result of the potential deterrent effects of the report outlined above, or an improved technical defence ability, or a different reason, it is still interesting to note;
- the media also revealed a certain helplessness of the government in politically responding to the case. The newspaper reports discussed indicate that the government had a tendency to downplay the attack and its impact: the data affected was considered less sensitive by the government than by MPs, and the government aimed at classifying the incident as industrial espionage while it seems evident from newspaper reports that this was espionage conducted by a state actor. This may indicate the delicacy of the case with respect to permanent neutrality: due to missing precedent with respect to permanent neutrality and cyberspace, the government did not want to cause a diplomatic incident (or even a straightforward attribution) which might cause an impact

on permanent neutrality practice. This impression of “downplaying” by the government is, for example, strongly backed by the parliament press release discussed in Subsection 5.3.4;

- finally, the problem of a missing option of “hack backs” is raised in a few newspaper articles: it is mentioned as a restriction that might be too strong since it prevents a further investigation of the case after its public disclosure. However, as stated earlier when discussing hack backs, Switzerland is neither restricted by neutrality law nor by its own legislation in conducting hack backs when deemed necessary. Nevertheless, conducting hack backs is only permissible when a cyberattack reaches a certain level of impact against Switzerland’s national interest (for example, impacting its critical national infrastructure), which was not the case with the RUAG Hack.

Some further findings have been provided by means of the case study: A conclusion from the points listed above may be that permanent neutrality has a counter-intuitively de-escalating effect with respect to the challenges brought forward by the cybersecurity dilemma. In particular when considering the potential effects of the publication of the RUAG Report: It provides a means of deterrent, while not escalating a diplomatic incident by means of a public “blame game”. As such, it provides an example of a very elegant response to the challenges outlined earlier in this chapter with respect to the effects of the cyberrevolution on the concept of permanent neutrality.

Furthermore, it is useful to consider what could have been different scenarios with respect to the events that occurred in this case.

First, a hypothetical case, where Switzerland implements an integral approach to neutrality provides a plausible counterfactual reflection: In that case only a minimal or no collaboration with respect to threat intelligence sharing would have occurred. Consequentially, the implementation of integral neutrality could have affected national security interests negatively.

Next, it is useful to consider the hypothetical option of not releasing the RUAG Report: In that case, no signalling would have taken place and, therefore, also no deterrent effect can occur. Furthermore, the zero-day methods used for the RUAG Hack could potentially still remain undisclosed to the general public (an other countries or large enterprises). With respect to Switzerland’s approach of fostering a collaborative

and multilateral approach towards tackling the challenges of cybersecurity (see Subsection 5.2.2), this might seem inconsistent: It would not contribute to Switzerland's trustworthiness as a permanently neutral party.

Furthermore, the case of an official attribution of the RUAG hack may be of interest: Such an official and public attribution might cause a diplomatic incident and lead to a public "blame game"; it would be against the permanent neutrality principle of attempting to be an *ami de tous* (see Chapter 4).

5.4 Conclusions for State Neutrality in Cyberspace

Throughout this chapter, the findings have been juxtaposed with the research questions of this thesis. First, Section 5.1 discussed theoretical implications for cyberspace that had emerged from the analysis and discussion of relative neutrality in Chapter 3. This already included some reflections on the applicability of neutrality law to cyberspace and reflections on some challenging scenarios. Also, reflections were provided on the potential implications of cyberspace on permanent neutrality, considering findings on conventional permanent neutrality from Chapter 4 and the conceptualisation of cyberspace and its challenges in Chapter 2. The theoretical discussion of the impact of cyberspace on the concept of neutrality was enriched by means of interviews. The section concluded by reflecting on the advancements made with respect to the research questions and conjectures of this thesis. It was concluded that while the follow-up questions (Question 1.1 and Question 1.2) had been addressed and the findings so far indicated that both Conjecture 1 and Conjecture 2 hold, further addressing of how neutrality is affected by the emergence of cyberspace is required. A particular finding was that, while relative neutrality seems to become less relevant on the background of the emergence of cyberspace, it remained unclear what this might imply for permanent neutrality.

Section 5.2 thereafter provided reflections on a few examples of permanent neutrality evolvments on the background of the cyberrevolution, in order to deepen the understanding of how permanent neutrality might evolve on the background of cyberspace. While these examples provided weaker indicators, the case study in Section 5.3 on the RUAG Hack case provided a case study on cyberspace, yielding insights on the specifics of how a neutral country can respond to an incident in cyberspace that is deemed unfriendly but does not cross the threshold of conflict. A major contribution of this thesis is the concept of "legal signalling" as both deterrent and de-escalative measure for neutral countries. The case of the RUAG Hack

further introduced the concept of indirect attribution by means of releasing obvious factual analyses without attribution: The attribution is done by the public, not the government. In this sense, the government of a neutral country can avoid being drawn into an inefficient “blame game” with the attacking country while still enabling attribution—the attribution is outsourced to the public discussion (e.g., newspapers) and only the technological facts and analyses are provided by the government. The release of technological details also has been found to have a deterrent effect: It signals a significant technological capability, which might deter a future attacker. Even more importantly, it imposes a threat on an attacker deploying zero-day attacks: The publication of a detailed technical report reveals a zero-day. The attack can thereafter no longer be considered a zero-day and other institutions or countries can prepare against a similar attack. An attacker will consider deploying an attack to a neutral country that publishes a technical report carefully, since the cost of deploying the attack is that it can no longer be used as a zero-day in future attacks.

The examples outlined in this chapter further signify a value of neutral countries also on the background of the cyberrevolution: Neutral countries can significantly contribute to international stability with respect to cyberspace by means of norms building, confidence-building measures, hosting international institution including protecting these institutions by means of providing a functioning cybersecurity ecosystem, or supporting international fact-finding such as by providing support for independent forensic analyses of state-level cyberattacks.

A main conclusion drawn from this chapter is that permanent neutrality arguably is seen to contribute to both national security and international stability. This conclusion is formalised by means of the following lemmas:

*Lemma 5.4.1. Permanent neutrality has evolved, on the background of cyberspace, towards emphasising *good services* and *balance of power*.* This lemma follows due to the indication of examples discussed in Section 5.2, namely Switzerland’s active approach towards norms building and cyber-diplomacy.

Lemma 5.4.2. It is permissible for a permanently neutral country, when following the approach of active neutrality, to engage in cyberthreat intelligence sharing with other countries, despite the ambivalence between CNA and CNE. This lemma is a deduction from the analysis of the RUAG Hack case. It is a manifestation of the principle that neutrality is a function dependent on national security interests and not vice versa.

Lemma 5.4.3. The response of a permanently neutral country to a state-backed CNE or CNA may, counter-intuitively to the cybersecurity dilemma, have a de-escalating effect, as has been demonstrated by the analysis of the RUAG Hack case and the respective public release of a technical report. As such, permanent neutrality may be seen to continue to contribute to national security as well as international stability. This lemma follows from the findings in Section 5.3. In particular, it includes the mechanisms of indirect attribution, publication of zero-days, and *show of force*.

Lemma 5.4.4. The permanently neutral's national legislation may provide for "legal signalling" as outlined in Subsection 5.2.3, which may have a de-escalating and, therefore, stabilising effect due to the predictability of the neutral country's deployment of CNA and CNE. However, discussions in the media and statements from interviewees also indicate that a permanently neutral might nevertheless require the ability of "hack backs". It is, therefore, questionable, whether the form of "legal signalling" outlined may be realistically upheld as an element of permanent neutrality when weighed up against national security interests.

Lemma 5.4.5. Overall, the indicators revealed by the research in this thesis point towards a continued relevance of the principle of permanent neutrality; the concept has evolved further based on the challenges posed by cyberspace and has revealed novel, de-escalating response mechanisms to common challenges posed by cyberspace.

Chapter 6

Neutrality as a Concept Beyond States

The aim of this chapter is to provide an example of how the findings on (political) state neutrality could be applied to other domains. For this purpose, it introduces the concept of *platform neutrality*, including a motivation, a definition, and an example of how such a concept could be implemented.

However, the aim is not to provide an in-depth analysis—or even a full case study—which fully evaluates the validity of the idea of platform neutrality. Rather, the this chapter should be understood as an epilogue on the potential applicability of findings on *state* neutrality to non-state actors given the background of the cyberrevolution.

A similar common application of the term *neutrality* is known under the term of *network neutrality* (or: *net neutrality*). Section 6.1 shortly discusses the relation of the term *network neutrality* to state neutrality: It explains, why network neutrality is not particularly related to ideas of political/state neutrality. Furthermore, it outlines approaches to the term of *platform neutrality* which are of an economic nature and should not be confused with the understanding of *political* or *social* platform neutrality stated in this thesis.

Thereafter, Section 6.2 outlines the general motivation for the concept of platform neutrality. This motivation is further backed by a more thorough discussion of some examples that emerged on social media platforms throughout 2020, which is provided in Section 6.3. Subsequently, Section 6.4 provides a deduction of functions for platform neutrality from the state neutrality functions outlined in Chapter 4. Furthermore, it formulates a definition of the term *platform neutrality*. Finally, Section 6.5 discusses different approaches to the question of how social media companies implementing platform neutrality could be governed.

The work in this Chapter strongly relies on two papers published by the author at double-blind peer-review conferences, both in 2021 [164, 165]. The respective papers may be found in Appendices C and D.

6.1 A Note on *Economic* Neutrality

The idea of technological neutrality is not new. The term of *network neutrality* has been introduced by Wu in 2003 [9] with a particular focus on the neutrality of Internet Service Providers (ISPs), in relation to the Internet traffic they route for users and content providers. Net neutrality bears an economic focus: ISPs should not favour traffic by specific content providers at the cost of other content providers and their users, in order to enable a free market of content. Furthermore, they should not restrict the use of their networks to specific application layer protocols, such as http(s) (for web browsers), streaming protocols (for services such as Netflix), etc. Rather, they should allow broad use of the Internet for all sorts of applications layer protocols.

Platform neutrality has also been discussed under an economical focus, for example, by the *Conseil National du Numérique* in a 2014 publication [166]: Platform Service Providers (PSPs), such as Google, Facebook, or Twitter, should remain economically neutral towards services they provide. Originally, some PSPs built services and subsequently favoured their own appliances running on these services, generating a distortion of free market rules.

Gao and Yang [167] relate the term of platform neutrality to net neutrality in their 2015 article. Krämer and Schnurr (2018) [168] specifically focus on how the EU should regulate the economic neutrality of PSPs. The latter argue that economic platform neutrality should not be regulated by imposing conditions of neutrality but rather by means of greater transparency in order to ensure a fair free market.

The introduced concepts in the literature on net neutrality and platform neutrality both argue with the fairness of the free market and effectivity of the services offered. While this focus on economic fairness ensures a prosperous development of markets, it neglects an important aspect that is imminent to the social nature of platform services: the platforms provide a global forum for users and institutions. Not only should access to services (such as advertisements) be fair for customers and users; the forum that allows discussion and promotion of opinions should also be *politically* fair (i.e., neutral) for all users. Such a call for fairness for the global forum provided by PSPs is underlined by claims that PSPs provide the foundation for users to act as a

fifth estate of liberal democracy, as has been suggested probably the first time by Bill Dutton in a 2020 article [169]. This suggests that PSPs might be new non-state actors that have gained relevance for global developments, which is similar to that of states in what this thesis refers to as the conventional system of states (see Chapter 2).

6.2 Motivation for Platform Neutrality

The global importance of social media and technology platforms has become more apparent than ever during the year 2020: On three occasions social media platforms, such as Facebook and Twitter, played their part in managing information and serving as a discussion forum:

1. The emergence of the Coronavirus pandemic has become a major element of discussion throughout 2020;
2. the Black Lives Matter movement has led to a broad and global discussion about racism and inclusion, which has also been led through platforms such as Facebook and Twitter;
3. the elections in the US in November 2020 have received significant attention on social media platforms, including the claims of election fraud following the election.

During times of “lockdown”, social media platforms have become tremendously important as a means for accessing news, communicating with governmental and other institutions and for political discussion. Bill Dutton described in 2020 [169] that Internet users form a fifth estate of liberal democracies: by communicating on-line, they multiply a local comment, statement, or other activity in its effect by sharing it with the broader public of the Internet. Social media platforms are essential providers for multiplying Internet users’ contents and, therefore, may be seen as an essential tool for the power projection of this fifth estate.

Due to negative experiences with “hate speech” and misleading or contradicting information, requests for censorship or stronger control of online platforms have arisen. However, the nature of cyberspace is inherently global and challenging for regulation. Companies affected are subject to a specific jurisdiction—in many cases, the US—but provide services globally. The inherent value of these platforms is that they are available globally and that they virtually bring together users and customers from different countries. Users share content, generate and consume information and participate in

discussions or use other services offered by the platform providers. Content is generated by platform “participants”. Creating a strict regime of regulation with many restrictions carried out on a national level would deconstruct the global character that makes these platforms unique. Some approaches have been made to overcome clear cases of criminal activities since these usually share the consensus and thus support of a sufficient number of countries. However, regulating content globally beyond such clear cases is a major challenge. Social media platforms such as *Facebook* or *Twitter* have initiated a regime of self-regulation, in order to address some of the resulting problems. These social media platforms offer a forum for global discussion with an impact on national politics and democratic procedures; how should these platforms relate to the state and how should they be controlled while ensuring their global character is not nationally compartmentalised? As Lucas Kello argued in his 2017 book *The Virtual Weapon* [8], these platforms should be considered an additional actor in the realist global system of states of international relations.

This thesis suggests that the challenges outlined might be addressed by means of the concept of *platform neutrality*, which is inspired by findings in this thesis on state neutrality and defined in the upcoming sections.

6.3 Examples of Social Media Developments in 2020

As outlined in Section 6.1, political and social aspects have barely been considered under the term platform neutrality. This section discusses three situations arisen in 2020 that have further substantiated the problems of regulation of global platforms. This is of particular relevance for liberal democracies, which rely on the ancient idea of a forum for free discussion. While such fora are conventionally controlled by means of national laws and enforced by the state, the global nature of online platforms introduces problems. An interesting predecessor of the social media online platforms known in 2022 was the *Public Electronic Network* (PEN) in the City of Santa Monica, discussed in an article by Schmitz et al. in 1995 [170]: While its aim was not global, it was nevertheless a successful implementation of a local Internet-based forum for the citizens of the City of Santa Monica. The social media platforms available in 2022, however, have a far more significant impact on societies, due to their global reach and their empowerment of individuals not just within a local sphere but with global reach.

6.3.1 Misinformation during the Coronavirus Pandemic

The emergence of the Coronavirus pandemic has led to “lockdowns” in Europe and the US from March 2020 onwards. These lockdowns have led to an increase in people working from home and, therefore, also relying more on online platforms for work and social interaction. Social media platforms have received increased attention as a consequence due to online discussions on topics connected with the pandemic. The spread of false information through Facebook has been subsequently declared a “major threat to public health” by a news article released in 2020 by AVAAZ [171]. Sites spreading misinformation have been found to receive four times more attention than the information spread by trustworthy sources, such as the World Health Organisation (WHO), as Stauffacher outlines in a 2020 news article [172]; Facebook’s algorithms have been found to favour misinformation. While Facebook has claimed to take action by means of warnings attached to potential misinformation campaigns, this has been found to be ineffective as it only flagged 16% of misinformation [172] in a study comparing its efficiency with that of independent human inspectors. This was perceived as contradicting attempts of Facebook and other social media platforms marketing themselves as supporters for tackling the global pandemic earlier in the year [173]. It has been pointed out, however, that the distinction between misinformation handling and censorship is delicate [173], and indeed PSPs have been criticised for restricting freedom of speech in an illegitimate way, even if this happened accidentally. For example, the Swiss website *corona-data.ch* had been blocked for linking in posts by Twitter at some point, even though the website’s contents were legitimate and trustworthy. Such unintended consequences fuelled conspiracy theories about the pandemic. Further efforts by social media companies included the launch of information centres that should provide unbiased facts, as has been documented by Hatmaker in 2020 [174]. Furthermore, a ban on specific ads, e.g., facemasks, was announced. Due to problematic posts and statements from politicians, social media platforms further started removing posts of publicly elected representatives, such as the Brazilian president Jair Bolsonaro (vide a 2020 news article by Thier [175]). This first-ever deletion of posts on the basis of misinformation was an important precedent. Later in the year, a similar precedent occurred with the first-ever deletion of a post by the US president, Donald Trump, also in connection with a post classified as misinformation (vide a 2020 news article by Kormann [176]). Facebook justified deletions by stating that they spread misinformation and infringed the platform’s guidelines. Youtube also took steps in connection with the pandemic to avoid the spread of misinformation: it introduced fact-check panels under videos relating to specific search

terms [176]. Twitter took a more radical approach by deleting accounts that spread conspiracy theories [176]. These examples emphasise the importance of establishing a mechanism to prevent unintended censorship.

The examples outline above motivate reflections on how these problems could be addressed: Should PSPs be regulated? If so: by whom? The US government could presumably regulate the PSPs hosted within its territory. However, this regulation might have a global impact: Do the PSPs located within the US have to adhere to the regulations also when providing services in foreign territories? And can countries that do not host the physical offices of a PSP also successfully regulate its contents? What if different national regulations differ? The services are usually provided globally and the inherently revolutionary character of these services is based on their global provision. Can PSPs still function as platforms for the fifth estate with global reach, if they would have to offer potentially strongly differing services depending on the physical location of their users? Could the PSPs be assigned some sort of neutral status, and, similar to an actively neutral country, implement some kind of neutral judge function based on a common set of principles, in order to limit a negative or even destructive impact of online movements, while not engaging in restrictive online censorship of political content on-line per se?

6.3.2 Reactions to the *Black Lives Matter* Movement

The second case example covers the *Black Lives Matter* (BLM) movement that gained public attention around May 2020, following the death of George Floyd. The case was heavily discussed on social media, fuelled by measures induced on society following the spread of coronavirus and the resulting increased use of the Internet for communication. The movement also triggered a discussion on discriminatory posts, hate speech, and verbal violence against minorities or suppressed groups on social media platforms [176]. Social media platforms first emphasised the aspect of free speech, but later experienced pressure from the public, their customers (i.e., organisations that pay for advertisements), and their own employees. Reddit banned accounts spreading hate speech, an action that has been labelled as “deplatforming”, followed by Twitter, Youtube, and Tiktok. This has been documented by a news Article written by Hurtz in 2020 [177]. Facebook, which had previously taken a less restrictive approach, declared that it would change its guidelines, following protests of its employees and threats from advertisement customers to withdraw their advertisements from the platform [178]. Twitter decided that it would delete posts or, in case they were against Twitter’s guidelines but from an author of public interest, such as the US president,

Twitter would hide them behind a warning message. The delicacy of the action taken by the PSPs should be underlined by some important considerations: The tension between the freedom of speech versus action taken against the spread of misinformation (often labelled as “censorship” by its contestants) has already been explained in the case example on coronavirus. The questions raised under the pressure of the BLM movement underline similar problems: While presumably the general goal of banning hate speech and verbal violence is widely shared, the line between what is and is not allowed to be posted is difficult to define and risks being subject to opinion bias or temporary waves, which could result in unfair discrimination of non-mainstream opinions in their right to free speech. The sequence of events with respect to the regulation of posts on the background of the BLM movement illustrates this problem: instead of basing its activities on general rules that apply equally to all actors, Facebook only responded to criticism emerging from one opinion group and gave way to pressure from employees and financial pressure from its advertisement customers. While it did resist governmental pressure, and so did Twitter when experiencing far greater pressure as a response to its ban of a post by the US president, a response to political pressures from opinion groups or financial pressures from advertisement customers does not yield an approach towards restricting verbal violence or hate speech that is applied equally to all users. Rather, it seems that Facebook exclusively responded to public pressure. Claims have been made that the public pressure Facebook responded to yielded a restrictive situation, in which harmless posts were banned [178]. This practice might favour a specific opinion and give way to claims of censorship and fuel conspiracy theories on information control.

6.3.3 The US Presidential Campaign in 2020

The third case on the US election campaign in 2020 has to be understood on the background of the BLM movement already described since it also became a topic in the US elections. The already discussed warning message displayed on top of one of the US presidents’ tweets resulted in a power battle between the US president and Twitter: The US president announced he would sign a decree in order to change the 1996 *Communication Decency Act* that disengages Internet platforms from any responsibility for the content generated by their users. It provides the basis for the business model of PSPs (as witnessed in the early 21st century) but, according to the plans expressed by Donald Trump, should be changed to ensure freedom of speech and prevent any “censorship” through PSPs “against conservative” opinions (vide a newws article by Langer from 2020 [179]). The decree did not materialise. Nevertheless, the

intervention of a political actor, the US president, in operational decisions of the platforms underlines their importance in the political process of Western countries and particularly the US. The case of the US elections is particularly interesting since large PSPs are mostly subject to US jurisdiction. Therefore, the US is the one country in the world with the greatest influence on PSPs' practices, potentially being able to restrict or even shut down PSPs located in the US. As such, the US is a country that can influence PSPs' practices globally by means of national regulation, while other countries struggle to effectively regulate PSPs since they are beyond their direct jurisdiction. There are mechanisms employed by states, particularly by some European states or also the EU, that influence PSPs and that companies adhere to in order to avoid difficulties. Nevertheless, states have limited scope in pressuring PSPs to comply with their regulations when acting on their own. The case of the US illustrates why PSPs might have to remain neutral from a state, in order to provide a political forum that is not subject to restrictions by a government; however, the emergence of hate speech and verbal violence also underlines that some sort of regulation seems to be required; PSPs have underlined their will to remain neutral from state content providers by flagging accounts that are connected to states or politicians: For example, Twitter has started to flag accounts of state-influenced or state-owned media, such as specific Chinese or Russian content providers, in order to ensure transparency of content provision (vide respective articles in NZZ [180] and SZ [181] from 2020).

6.3.4 Suggestion of Mitigation Mechanisms

Having illuminated three cases and the connected problems, this subsection discusses some mitigation mechanisms.

First, Facebook explained that it will address problems of political advertisements early in 2020: Whoever would want to place such advertisements would need to undergo an additional registration and verification mechanism (vide a news article written by Muth in 2020 [182]). These measures were aimed at increasing transparency by introducing an advertisement archive. They were inspired by experiences from previous elections and popular votes, such as the 2016 US presidential election, the Brexit popular vote in the UK, and the Irish referendum on abortion. The measures were aimed both at the US election and the EU elections in May 2020. One main focus was to prevent so-called *Dark Ads*, which are only displayed to very specific user groups and, therefore, bear the potential for misinformation while remaining hidden from broader public attention and scrutiny. The advertisement archive would make it

possible for the public to trace political advertisements and access information such as the issuer's identity, the amount paid, and who an advertisement was targeted for. This new practice is in line with PSPs acting as a global forum by increasing transparency and accountability, elements that are essential in the non-digital political discussion in liberal democracies. However, they raise important questions: is it sufficient that PSPs self-regulate? Who determines how far this regulation goes? Is there a need for democratically or otherwise legitimated control of measures taken? Are these approaches applicable independently of varying approaches towards information protection or privacy? Some societies might perceive publicising information about funders as questionable practice with respect to privacy and information protection rights.

While the discussed transparency and accountability mechanism for political advertisements inherently implies Facebook sees itself as a political forum of high relevance, Facebook announced a ban for political advertisements during the week preceding the 2020 election date in the US [183]. The cited publication also defined clear (mis)information policies applied to statements on COVID-19 risks during the election, posts that might attempt to delegitimise the election's outcome or premature claims of victory. These measures were probably inspired by concerns about the potential unrest such misinformation could cause in the political process. Similar measures would conventionally be considered within a state's legal code concerning the election process. However, in this case, the measures were imposed on a purely self-regulatory basis. Due to the turbulences around the election result in the US, Facebook announced to further extend the ban on political advertisements and its other measures in order to avoid confusion during the process of the handover of power (vide news articles written by Hatmaker [174] and Kamps [184] in 2020). The importance of these measures in terms of political stability and avoidance of the spread of misinformation and conspiracy theories has been emphasised by Kamps in his 2020 news article [184]. These measures, however, did not stand under any particular national legislation. The cascade of events and actions outlined emphasises Duttons' 2020 argument [169] of PSP users acting as a fifth estate through the globally available political and social fora. They also reveal the potential dependence on the goodwill of PSPs when they are beyond a state's jurisdiction. The "power struggle" between PSPs and the US president on the handling of questionable posts made by the latter, as documented by a 2020 news article written by Denkler [185], emphasise these aspects, while also underlining the need for PSPs to be somewhat independent of governmental influence.

A further attempt to resolve the regulation problem has been taken by US lawmakers in November 2020: the heads of PSPs, such as Facebook and Twitter, had to answer questions during a hearing in the US Senate. Both Mr Zuckerberg (Facebook) and Mr Dorsey (Twitter) emphasised that reform to legal mechanisms of content moderation might be required. They further stated that they implement different measures for content moderation, as documented by a news article written by Isaac in 2020 [186]. Twitter was more restrictive, banning accounts more quickly than Facebook. The tension between verifying information in order to avoid misinformation and providing a free and open forum under the principle of freedom of speech is handled differently; it is not supported by any national legislation. PSPs have come to the conclusion that some moderation is necessary on the background of the events outlined earlier, as has been outlined in a 2020 NZZ news article [187].

While the self-regulatory measures outlined might be seen as a mitigation for the problems, the success of these measures is questionable. Reports have shown that accounts that had been banned from the most popular PSPs later reopened on other, less restrictive PSPs: a platform called *Parler* specifically marketed itself as being less restrictive towards content and attracts mainly right-wing and conservative users and content providers, as has been documented by a news article written by Thier in 2020 [175]. Parler claims to offer “real” freedom of speech while rejecting “technofascism” [175]. However, this practice of Parler also gave room to misinformation and conspiracy theories, such as posts about an alleged “plan-demic” being the explanation around the coronavirus pandemic. Parler’s community guidelines leave scope for interpretation and give precedence to the principle of freedom of speech in case review volunteers disagree. Such loose enforcement of guidelines bears its problems.

The importance of some kind of regulation is underlined by the case of verbal violence and misinformation against Kamala Harris: Facebook had to remove posts about US vice-president-elect Kamala Harris that were perceived as “verbally violent”. Facebook took the approach of deleting the posts, while not banning the groups that had allowed the spread of such posts (vide a news article written by Clayton in 2020 [188]). The emphasis lies on moderating the content depending on specific criteria, while not generally banning users or groups from using a platform. As such, Facebook acknowledges the necessity and openness of its role as a global forum but restricts some of the content in case it is too violent or breaches the limits of its hate speech definition. Facebook has introduced a further mechanism to ensure the political independence of its content moderation decisions, which might be

a first step towards implementing political platform neutrality: the Facebook *Oversight Board* provides users with an option for appeal content moderation decisions (vide a news article written by Levy in 2020 [189]). It has been called “*Facebook’s Supreme Court*” [189], providing para-state structures in terms of a judiciary for content moderation. Mark Zuckerberg has claimed “*Facebook should not make so many important decisions about free expression and safety on our own*” and Facebook further admits that “*with our size comes a great deal of responsibility*” [189]. The board’s members are funded by means of a separate Oversight Board Trust, which ensures the members’ financial independence from Facebook [189]. The board’s structure further prevents a national or cultural bias by involving members from more than 27 countries, speaking more than 29 languages [189]. An example from the EU shows how transnational collaboration further enhances self-regulation: Meta Beisel and Kolb (2020) [190] outline the reaction of the EU Commission’s Vice-President, Věra Jourová, upon identifying foreign powers, such as Russia and China, as being responsible for specific misinformation campaigns: the EU Commission now asks PSPs to provide a detailed monthly report, which outlines their self-regulatory activities. This ensures transparency and freedom of speech. Notably, even the Chinese-owned video platform Tiktok participates in this voluntary process. The EU’s initiative provides an interesting example of transnational control, with an emphasis on transparent self-regulation, while providing little actual regulation; the EU takes an approach of non-regulation through transparency and potential of negative consequences in case the mitigation mechanisms are insufficient, i.e. it expects the PSPs to regulate themselves and provide detailed documentation about the mechanisms of self-regulation. Due to the EU’s structure, this oversight is democratically legitimized while omitting direct governmental or regulatory influence.

6.4 Definition of Platform Neutrality

The concept of political and social platform neutrality is inspired by state neutrality. PSPs, functioning as global actors, should be neutral from specific countries and political or social groups.

The functions of platform neutrality illustrated in Figure 4.2 are derived from the respective functions of state neutrality as defined by Riklin in 1991 [5], which were presented in Chapter 4. The illustration of functions from the respective subsection is depicted in Figure 6.1 as an aide-mémoire. The adapted functions for platform neutrality are introduced in the following and displayed in Figure 6.2.

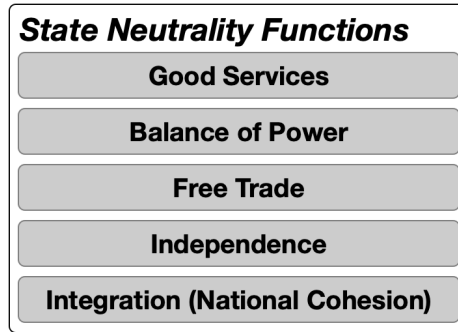


Figure 6.1: The functions of permanent neutrality, as defined by Riklin in 1991 [5] and presented in Chapter 4.

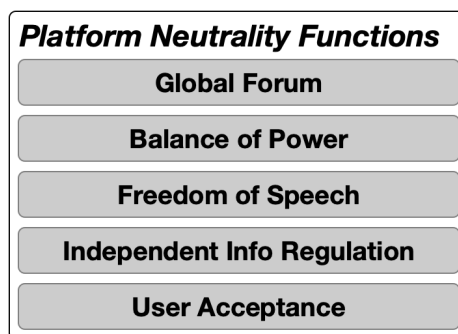


Figure 6.2: Platform neutrality functions, adapted from Stolz' definition in 2021 [3].

User Acceptance describes the requirement of neutrality for a broad user base. Users who feel that the platform they use supports a certain political view or narrative will not trust this platform and boycott its use by switching to a different social media provider. However, the value of social media platforms is derived from their universality: only when they provide a space considered equally open to any political groups and individuals, the platforms may function as a *global forum*—i.e., a space where people from all around the world can multiply their voice globally as Internet users in the sense of Dutton’s fifth estate (see article by Dutton in 2020 [169]).

Furthermore, the platforms themselves have an interest in appealing to the broadest possible user range due to economic incentives. Similarly, users will be inclined to use a platform that most of their friends use since they aim to connect with all of their friends through the same platform. In this sense, user acceptance might be considered a similar principle to state neutrality’s integration function.

Independent Info Regulation denotes the possibility to detach information regulation from the control of a government or state. In order to avoid censorship or the control of media and information—as considered necessary for liberal democracies—the information should not be controlled directly by a state. Conventionally, the oversight over information control mechanisms would lie with a judiciary system, following a state’s legislation. However, on a global platform, such as social media, such a mechanism has a limited impact: While social media platform providers may be forced by national legislation to abide by local (information) legislation, in practice, users may easily circumvent such legislation if policies are only based on geo-blocking and not applied universally by a social media platform provider. It is therefore more reasonable if platform providers define and implement rules and principles for the contents that may be shared on their platforms globally and in a self-regulated manner, relying on a broad consensus of countries.

This also prevents a single state from controlling online information and ensures freedom of information, while maintaining a basic set of principles, for example, to avoid hate speech or misinformation. Hence the function of *Freedom of Speech* of platform neutrality.

The *Balance of Power* function relates both to its counterpart in state neutrality in terms of balancing power on a global level as well as within a state: On the one hand, neutral platforms may act in balancing power between states, since they provide a forum and define the rules for contents that users (including state entities or members of government) may post. On the other hand, this also provides a balance

within a state, between entities such as the populus and a government, which would traditionally have been regulated by means of national legislation.

Global Forum, finally, is closely related to the balance of powers: neutrality enables platforms to provide global forums for people globally on an inter- and intra-state level.

Therefore, platform neutrality may be formalised by the following definition:

Definition 6.4.1 (Platform Neutrality). ***Platform neutrality denotes the application of political neutrality principles to social media platforms.** Specifically, it denotes that a social media platform is neutral with respect to freedom of expression or political opinions. However, similarly to the concept of active neutrality for states, this does not imply a rule-less or anarchical environment. Rather, the politically neutral platform should apply previously defined rules for content management in an objective manner and without following an agenda of its own with respect to political opinions/discussion. A neutral social media platform should define structures for the definition of such rules as well as internal, independent bodies to which content moderation decisions may be appealed.* The latter is inspired by Facebook’s *Oversight Board*.

Lemmas are not formulated in this chapter, since its main aim is to demonstrate how state neutrality concepts could be transferred to non-state actors on the background of the cyberrevolution. However, future research may suggest that specific structures or mechanisms are particularly suitable for implementing platform neutrality as a concept. Furthermore, it also seems plausible that lemmas might reflect on why it may make economic sense for a social media platform to implement platform neutrality.

6.5 Discussion on Governance

Naturally, the governance of such social media platforms raises questions: The envisioned role of social media platforms is somewhat coequal to that of states—traditionally, a state would provide an environment that ensures both freedom of press as well as protection from misinformation in conventional media, such as newspapers. The function of platform neutrality is to balance power within a state and among states: No single state should govern the rules among which neutral social media platforms operate. Various models come to mind with respect to how such a platform could potentially be governed without being dependent on one single state:

First, purists of free market idealism might envision that market pressure ensures that platforms evolve as neutral entities and implement an objective and fair mechanism, as envisioned by Definition 4.4.5. After all, users will migrate to the platform that offers the best service and platform neutrality serves the function of *User Acceptance*—therefore, the market will automatically push social media platforms towards a sensible implementation of platform neutrality entailing reasonable, objective content moderations.

Second, democracy idealists might envision that the users of social media platforms should have a say in the governance of social media platforms, maybe in a similar fashion as shareholders of a company. They could influence the culture and governing principles of a social media platform company, as well as the structures. Since the users would be spread across the whole world, no single government or country would dominate the network and the transnational/global aspect of social media platforms is respected by this form of governance. The question, however, remains as to what enterprise legislation such a company structure would rely upon: Would the users take the role of conventional shareholders? Or would a change in legislation be required in the host country of a PSP—and if so, which country should serve as a host; maybe a neutral country?

Finally, a multilateral body, similar to a UN institution or a transnational body, such as the EU, could engage in the governance of social media platforms. Such a form of governance would respect the global aspect of social media platforms while also respecting the conventional structures of national governments. Of course, a follow-up question would be the granularity of governance: Would such a multilateral or transnational governance approach require very specific rules and regulations and a high level of scrutiny? Or would the social media companies be granted a higher level of independence under the expectation of due diligence with the option for the multilateral/transnational body to intervene? Such approaches are, for example, being discussed and tested by the EU with its *Digital Services Act* (DSA) (vide a news article released by SZ in 2021 [191]) or, in 2023, with the EU’s discussions on regulating AI.

6.6 Conclusions on Platform Neutrality

As has been stated in the introductory paragraphs of this chapter, the aim was specifically not to provide a full-depth case study on platform neutrality or social media companies and the related problems with respect to misinformation and regulation.

This chapter introduced these challenges on the background of examples from the Coronavirus pandemic and events surrounding the US presidential elections in 2020—and provided a motivation for reflections on how to resolve these challenges on the background of the secondary research Question (Q2, as introduced in Chapter 1): The revolutionary character of social media platforms was discussed, referring on the unique character of the Internet and the multiplication of users’ influence through on-line means, characterised by Dutton in 2020 as the fifth estate [169].

A potential solution to the challenges might be provided by modern governance solutions and by the understanding that social media platforms do not only have a transnational character in terms of their global impact but also require supranational considerations with respect to the challenges this brings about. Platform neutrality was introduced as a means of reflecting the functions social media platforms might bring about—and also as governing principles that might affect the courses of actions of PSP. While platform neutrality is a theoretical construct, it is a contribution for understanding the factors that drive the PSP regulation discussion and provides the basis for discussing potential ways ahead in terms of supranational governance.

By introducing and discussing the concept of platform neutrality, this chapter has also provided insights into what was introduced as the potential argument of this thesis in Chapter 1: Namely, that the concept of neutrality, as discussed, refined, and advanced in this thesis, may also yield relevance for applications and discussions of its central ideas beyond states. In doing so, neutrality has been shown to be of some value in a more general sense: as a theoretical ground for reflection for challenges posed by novel, or even revolutionary, challenges posed to societies on the background of the cyberrevolution. This also provides a positive indicator with respect to answering the secondary research question: The concept of neutrality may be considered as relevant beyond states, and in that sense, is relevant and an up-to-date concept with the potential of being further developed for applications beyond the state.

Chapter 7

Conclusions and Future Work

The preceding six chapters have outlined an evolution of the concept of *neutrality*. While Chapter 1 outlined the topic of this thesis, presented the research questions, conjectures, and arguments, reflected on the methodological difficulties of interdisciplinary research, and presented the research methods applied in this thesis, Chapter 2 pursued understanding the characteristics of cyberspace from different disciplines' perspectives. It also provided a first impression of what neutrality may refer to. As such, it already illuminated the follow-up questions of the central research question: It provided a foundation for understanding cyberspace and a first illustration of what neutrality is.

The subsequent chapters engaged in thorough analyses, case studies, and discussions on different “types” of neutrality: The principles of relative, permanent, integral, differential, and other neutralities were analysed in existing research and systematically defined, set into relation to each other, and a taxonomy was developed. Overall, *neutrality theory* was defined and advanced through the findings in these chapters and the formulation of definitions, lemmas, and conclusions: Chapter 3 provided a first discussion on the applicability of relative neutrality law to cyberspace scenarios. Thereafter, Chapter 4 focused on thorough case studies on permanent neutrality and active neutrality, since the academic literature on neutrality does not provide a comprehensive taxonomy and theory.

Chapter 5 provided major contributions to advancing answers to the central research question and the specific research questions. With respect to the secondary research question, strong indications exist that neutrality still appears to be an up-to-date concept, even on the background of cyberspace. The discussions of the RUAG Hack (see Section 5.3) and further examples outlined (see Section 5.2) indicate how permanent neutrality has further evolved on the background of cyberspace and provide highly valuable insights; the latter form the main pillar of the *Central Argument*

(see Chapter 1). The “epilogue” on platform neutrality in Chapter 6 further supports that statement: Neutrality may be adapted for non-state actors and, thus, underlines the plausibility of Conjecture 3 and outlines the *Potential Argument* formulated in Chapter 1.

In the upcoming sections, some final conclusions are drawn: Section 7.1 outlines this thesis’ major contributions to advancing knowledge in a more general sense, i.e., beyond the research questions outlined in Chapter 1. Section 7.2 outlines some possible avenues for future work.

7.1 Conclusions

This thesis has been successful in illuminating the research questions outlined within it and the findings may also be considered to contribute to various fields of research in a broader sense:

First, this thesis identified the lack of comprehensive academic literature on the concept of (state) neutrality in a broader sense. In particular, the author of this thesis found no comprehensive *theory* of neutrality, that could integrate the different “types” of permanent neutrality and outline generally applicable, guiding principles. Furthermore, a holistic overarching understanding of how relative and permanent neutrality complement and influence one another was not found to exist. The author of this thesis hopes that this thesis may provide a significant contribution to a thorough and systematic understanding of *conventional* neutrality theory. In fact, the reflections on conventional neutrality, though they may in the context of this thesis be considered as a mere prerequisite for addressing the evolvement of neutrality on the background of the cyberrevolution, form a fundamental contribution of this thesis to the academic understanding of conventional neutrality. The theory has been shown to be applicable to the most recent developments challenging neutrality in the context of the Russian invasion of Ukraine: Intuitively difficult to understand decisions of the Swiss government, such as the participation in economic sanctions or the condemnation of the Russian invasion in Ukraine can be explained by means of the framework provided in this thesis.

Furthermore, the thesis derived broad conclusions for the various interpretations of the applicability of relative neutrality (i.e., international neutrality law) to cyberspace—plausible interpretations were discussed, and less well-backed claims were identified and dismissed. This contributes to the advancement of a more general understanding

of how neutrality law should be understood, also in the public debate in Switzerland and internationally.

The thesis provides a substantial and independent contribution to the advancement of knowledge of neutrality law, as discussed in the Tallinn Manuals. Some claims in the Tallinn Manuals have been shown to be used by other authors as facts without further critical scrutiny or thorough reflection. This thesis contributes to a more critical understanding of how neutrality law is applicable to cyberspace and suggests plausible and technologically justifiable cases and interpretations of neutrality law in cyberspace.

The thesis introduced some novel aspects to the cybersecurity dilemma, which forms a very prominent theory in the field of international relations. These considerations might be received by the community of researchers in international relations as welcome examples of how cyberspace is not “doomed” to escalate conflicts. Again, an essential contribution to the academic discussion was provided by identifying and defining the concept of legal signalling and its de-escalating impact with respect to the concerns voiced by the cybersecurity dilemma; legal signalling was also found to have a potentially deterrent effect. Examples also illuminated how neutrality might have a positive impact on norms building, confidence-building measures, the cybersecurity of international organisations hosted in neutral countries and the potential role of the neutral host country, as well as potential contributions of neutral countries to international cybersecurity by means of supporting fact-based forensic investigations of intra-state cybersecurity incidents.

The case study on the RUAG Hack provides a further major contribution to the academic field of cybersecurity and the understanding of neutrality in that context: The thesis revealed how indirect attribution is a suitable tactic for a government that does not want to engage in direct attribution, in order to not compromise its trusted and neutral status while still responding to unfriendly cybersecurity activities emerging from states. Possibilities for de-escalating deterrents that may be implemented by neutral countries were identified: The release of a detailed technical report of an attack was found to be useful not only for indirect attribution but also for a demonstration of cyberdefence capability in the sense of a “show of force”, which may deter future attackers. The publication of a detailed technical report has also been found to deter, since it may deconstruct zero-days that have been deployed: An attacker needs to carefully evaluate whether the cost of having a deployed zero-day publicised pays off when attacking a neutral country.

Many aspects discussed in this thesis bear particular relevance for Switzerland as a permanently neutral country. However, during personal discussions of the author with some representatives of the Swiss administration, the challenges brought about were first very long neglected, only to be addressed later in a hasty, unreflected, and uninformed manner. This thesis may also be a source of advice and support for members of the Swiss administration, politicians, and the general public with respect to discussions on neutrality—both on the background of cyberspace and generally.

Finally, platform neutrality was introduced in an epilogue on the applicability of neutrality concepts to large technology companies or, more specifically: to social media companies. Contemporary problems, which are covered in sometimes very heated discussions in conventional and social media, might be addressed and (partially) resolved by means of the insights into neutrality provided in this thesis. As such, the thesis demonstrated how reflections applicable to state neutrality may well be useful as a foundation for new neutralities beyond the state.

7.2 Future Work

Naturally, many more things remain to be said, cases could be studied, examples outlined and concepts designed with respect to neutrality and cyberspace. Some ideas for further research are outlined in the following.

First, Switzerland's engagement in cyber-diplomacy and norms building, which has only been documented as an example in this thesis, deserves a full case study (or even multiple) in order to illuminate the various aspects of Swiss diplomacy and how it is affected and affects permanent neutrality.

Next, an aspect not addressed in this thesis is the idea of *data embassies*: What would happen if a foreign government asked a neutral country to “safeguard” its critical assets, servers, its central information systems or core data? Is a system similar to the Swiss banks imaginable with respect to digital data and systems located in cyberspace? How would this be technically implemented and what would the implications of international law be? Would such a hosting be compatible with neutrality law and principle neutrality?

A further topic that this thesis touched on and that deserves further illumination is *intelligence collaboration* of neutral countries with third parties: How far may it go? Where are its limits? When does it impact permanent neutrality in general? What about integral, differential, or active neutrality: how do the boundaries of what is

acceptable differ? Similar questions may, of course, also be asked with respect to defence collaboration.

Finally, the concept of platform neutrality was covered in an epilogue; it could as well fill one (or several) DPhil theses—its further investigation is strongly advised due to its topical relevance. In particular, recent events on Twitter / X and regulatory ambitions of the European Union with respect to the neutrality of AI provide for very interesting applications of the “*neutrality concept*”.

Unfortunately (and, maybe also: fortunately!), the scope of a DPhil thesis is limited—the interested reader is strongly encouraged to engage in further research on the topics outlined above or beyond.

Appendix A

Published Paper: *On Neutrality and Cyber Defence*

The following paper [43] was accepted as a submission to the 2019 *European Conference on Cyber Warfare and Security* (ECCWS, ISSN: 2049-9870). It was presented at the conference in June 2019 and published in the conference's proceedings. Additionally, a poster with the title *A Digital Red Cross? Potential of NGOs and Neutral Countries in Cyberspace* has been accepted for presentation at the conference.

On Neutrality and Cyber Defence

Marcel Stolz

Centre for Technology and Global Affairs (CTGA) / Cyber Security Analytics Group

University of Oxford, United Kingdom

marcel.stolz@oriel.ox.ac.uk

Abstract: Neutrality is a concept of international law, which the Swiss Confederation adopted in 1815. Its current idea goes beyond the legal requirements set by The Hague Convention of 1907. The convention comprises mainly of territorial definitions relevant for conventional warfare. Switzerland, on the other hand, defines the idea of neutrality more broadly. Considerations on its cyber neutrality policy could also be applied to other countries that claim to be neutral or impartial. We take Switzerland as an example for a case study, as it has the longest continuous tradition of neutrality.

Due to the non-territorial character of cyber conflict, the conventional practices of Switzerland's neutrality and foreign policy are confronted with challenges: Major challenges are posed by the clash between national interest and the self-restrictions of neutrality policy. The national interest demands a strong cyber security capacity and an effective defence capability. However, this might only be achieved by means of international collaboration and knowledge exchange. This collides with the principle of impartiality and non-intervention in international conflict, a core-concept of neutrality.

A new concept for neutrality in cyberspace has to be developed, which builds on the foundation of Switzerland's tradition as a neutral country in the international community. This paper outlines the inherent problem of neutrality and cyber defence. We describe Switzerland's neutral tradition, how it has developed since 1815 and its current characteristics, described as *active* neutrality policy. Furthermore, we illustrate Switzerland's involvement in cyber activities and outline where these involvements reach their limits. Finally, an outlook on future implementations of neutrality policy is made.

Keywords: Neutrality, Cyber Defence, Switzerland, Cyberspace dilemma in kinetic warfare

1. Introduction

Neutrality of a state or nation is a concept of *conventional* or *kinetic* warfare. Its initial implementations have developed on the basis of informal practices of non-aligned states. A legal definition of neutrality has been adopted in international law by The Hague Convention (1907). While the convention codifies the rights and duties of neutral nations in war on land and sea, it does not cover all aspects of neutrality. In particular, there is no generally accepted legal codification of the rights and duties of neutral nations in cyber conflict. With the emergence of conflicts in cyberspace, it is of vital interest for neutral nations to find a common understanding of the implementation of neutrality in cyberspace. Neutral nations need to know what is expected from them in this new domain of conflict—and what they may expect from the status of neutrality. Hence the motivation of this paper to cover neutrality with a focus on cyber defence.

When seeking solutions for a common definition of neutrality in cyberspace there is more to take into account than a legal definition of neutrality in conventional warfare. The history of implementation and practice of the foreign and security policy of neutral nations has to be considered, since neutrality existed already before its legal definition. This implementation has changed over the centuries and provides material for case studies of neutrality, which can lead to a more thorough understanding of what state neutrality means. We refer to this history of the implementation as *neutral tradition*.

1.1 Paper Outline

In this paper we investigate which steps are required in order to raise the idea of state neutrality to cyberspace. We do this by means of a theoretical analysis of neutrality policy on the one hand and an analysis of current approaches to cyber defence theories in international relations on the other hand. Since the most prominent and longest continuous example of a nation's successful implementation of neutrality is found in Swiss history, we mostly rely on examples and case studies related to Switzerland. As a framework of thought in cyber studies we mostly rely on the work of Lucas Kello (2017), as it provides a thorough analysis of the contradictions between classical defence thinking and the nature of cyber conflict and extends international relations theory to the domain of cyberspace. It is briefly introduced in Section 2. In Section 3, we analyse work on the neutral tradition and explore the case of Switzerland's implementation of neutrality. This will include frameworks developed for considerations on neutrality as well as challenges that neutrality policy had to face and prevail in the past.

Thereafter, Section 4 discusses some straightforward examples of Switzerland's reaction on cyber incidents in recent years. Building on the findings from Sections 2,3, and 4 we deduce and explain challenges that current neutrality policy has to face with regard to cyberspace in Section 5. Finally, Section 6 concludes and outlines possible future work on the topic of neutrality policy and its implications on cyber defence.

2. Cyber Studies in Political Science

Since the field of international relations, which commonly describes interstate conflict and cooperation, does not reflect adequately the nature of cyberspace—in particular its pervasiveness—Kello expands international relations theory in order to incorporate the *virtual weapon*., i.e. the effect of cyber operations on the International System. He claims that the virtual weapon fundamentally disrupts the *Conventional Model* of states as the dominant units of international relations theory. While the Conventional Model relies on a Clausewitzian approach to international conflict, Kello declares that he expands theory to post-Clausewitzian considerations. We believe that his analysis of technological revolution and its influence on global conflict provides a thorough basis in order to explain the challenges to conventional neutrality policy. The conventional theories of international relations neglect the novel character of the virtual weapon.

Kello defines third-order, second-order and first-order technological revolutions and analyses their effect on the Conventional Model. We shortly outline the basic concepts of these revolutions:

Third-order technological revolution, also known as systemic disruption, refers to “important adjustments within the sharp limits of the states system”. While the rational order of the International System is affected, the moral order is not. An example of systemic disruption is “the replacement of one or a group of dominant states in the system by another”. The basic mechanisms of the states’ contest for power are not changed.

Second-order revolution, also known as systemic revision affects the moral order of the International System. It maintains the Conventional Model: A state or group of states repudiates the “shared basic purposes of the units and rejects the accepted methods of achieving them, in particular restraints on the objectives and means of war”. Nevertheless, “it leaves the system’s organising principle, or state supremacy, intact”. Examples are the emergence of Soviet communism and its idea of world revolution or the strive for permanent peace as a founding principle of the European Union.

First-order revolution, or systems change, finally, overthrows the mechanisms of the Conventional Model in that it challenges the supremacy of states. Examples are alien (i.e. non-state) actors who try to dominate the actions of conventional states by means of new mechanisms of influence and power. It yields an altogether new type of International System beyond the concept of the supremacy of states.

We argue that this classification of types of revolutions is essential to describe the challenges of cyberspace to neutrality policy. A consequence of this systems change is the state of *unpeace*: While nations are not formally at war with one another, their hostile activities in cyberspace do not correspond to the conventional understanding of peaceful co-existence either. A further aspect of this systems change is the *diffusion of power*. In a system where states no longer hold the supremacy of power, other actors and groups have increased means of power to influence the actions of states. As states no longer hold the monopoly of power, defence is also fragmented: private (and other) actors, which used to be subunits of states, develop their own defence mechanisms in order to secure their interests. This further erodes the supremacy of states, as large technology firms gain influence not only in the defence of their own systems but also in the balance of cyber power.

A particular shift in defence thinking with effect on neutrality policy is the irrelevance of territoriality and the pervasion of dimensions of warfare. This aspect is partially introduced by Joseph S. Nye (2011) when he defines the nature of *cyberpower*. This novel aspect of warfare has yet to be fully understood and applied in military strategy. In cyberspace, most countries have a virtual border with most other countries and are, therefore not only vulnerable by means of a violation of their territorial borders but directly through cyberspace. These factors have an impact on conventional neutrality policy.

3. Switzerland's Tradition of Neutrality Policy

In order to understand more clearly the traditional implementation of neutrality policy, we outline the theory of neutrality policy in the upcoming subsections. We do this on the example of Switzerland, as its history provides the majority of interesting cases and Swiss neutrality is the longest example of a continuous and successful implementation of neutrality policy. It has lasted for over 200 years now. We first briefly outline the history of Switzerland's neutrality. Thereafter, we discuss thought frameworks and terms of neutrality policy. Finally, we illustrate Switzerland's current approach to neutrality policy within the Conventional Model. The content is mostly based on Suter (1998), Riklin (1991) and Holenstein (2014).

3.1 A Very Brief History of Swiss Neutrality

Some historians have claimed that Swiss neutrality policy goes back as far as 1515 (Bonjour, 1946). It is arguably the year of 1515—following the event of the *Marignano Defeat*—which marks a turning point with regard to the involvement of the Swiss states in conflicts outside their territory. The Swiss states continuously refrain from fighting in foreign conflicts during the following centuries and take measures to avoid being drawn into foreign conflicts. However, the actual starting point of Swiss neutrality is the year 1815, following the Vienna Congress and the Treaty of Paris, as is generally accepted by contemporary historians (Suter, 1998). Switzerland's neutrality was defined as *permanent*. This neutrality was challenged several times. Suter (1998) provides an essay highlighting some precedential situations. Neutrality was not only chosen by the Swiss but rather imposed by the great powers of Europe during the process of reorganisation after the Napoleonic wars. Switzerland's neutrality was based in its geostrategic location at the centre of Europe and the inability of the superpowers (Prussia, Russia, England, France and Austria) to decide who this geographically difficult terrain should be assigned to. This highlights an important precondition for neutrality: It cannot merely be chosen by a country. Neutrality has to lie in the interest of a majority of influential powers.

The underlying principle of neutrality is to *prevent bias towards any belligerent power even before a conflict is recognisable*. This goes beyond the legal definition of neutrality, which only covers the declaration of neutrality in an already ongoing conflict.

Suter explains the different nuances of neutrality over time. During the 19th century, neutrality was a means for sovereignty of a lone and yet very young liberal and direct democracy surrounded by mostly monarchic states. It was challenged several times when Switzerland had to mobilise its forces to deter a Prussian / German invasion, e.g. in the *causa Wohlgemuth*: Switzerland functioned as a safe hideaway for political dissidents, for example the German social democrats after Bismarck's anti-socialist laws were passed. From this time arises the principle that neutrality should not only be permanent but also *armed* in order to prevent or deter attacks. A neutral nation cannot rely on any foreign power to protect its interests. Its army has to be of substantial size and self-dependant. It is noteworthy that even in 1998 the only armies of larger size on the European continent were those of Russia, Ukraine, Turkey and France (Suter, 1998).

Armed neutrality became particularly important during the world wars. During the First World War, Switzerland experienced a strong ethnic divide and had to remain neutral in order to prevent internal instability. After the First World War, Switzerland chose to join the League of Nations, marking the start of what is known as *differential* neutrality: In respect of Switzerland's neutral status, Switzerland to participate in economic sanctions only, military sanctions of the League were ignored. Switzerland returned to its *integral* neutrality in 1938, leaving the League when it became obvious that it had failed its goal of collective security.

Swiss neutrality in the Second World War was far from perfect. Secret consultations between the Swiss head of armed forces, General Guisan, and the French general staff covered the case of Germany circumventing France's Maginot line through Switzerland. A German invasion would be a breach of Swiss neutrality, yet the consultations themselves were as well. Suter justifies them with the absence of alternatives and the presence of an imminent and existential threat. Minor breaches with regard to trade politics followed: Switzerland was forced to collaborate economically with the axis powers. Suter concludes that neutrality was one of several factors for relative peace, the other being: the usefulness of the functioning Swiss economy for the axis powers, the mobilised army, the ideological resistance (*geistige Landesverteidigung*), the humanitarian and diplomatic services for all belligerent powers and the luck of not being at the geostrategic centre of the war.

On this background, Switzerland pursued its strategy of integral neutrality throughout the Cold War. It would not join the UN, it would not participate in any economic or military sanctions and it would remain highly armed and provide diplomatic and humanitarian services for the international community. The Cold War shaped the still applied principle of *courant normal* in the case of economic sanctions: In order to not upset the sanctioned nation, Switzerland would not participate in sanctions. Yet, in order to avoid upsetting the sanctioning nations, it would also not allow any circumvention of sanctions by freezing its economic interactions to the *regular scope* of economic trade with the sanctioned country. Only after 1990 Switzerland started to integrate more into supranational institutions, joining the UN in 2002 and participating in UN economic sanctions. Early in the 21st century, Swiss Foreign Minister Micheline Calmy-Rey coined the term of *active* neutrality. It emphasises the responsibility of a trusted third party in peacekeeping processes. Micheline Calmy-Rey decided that Switzerland should become more active in foreign politics by means of expressing discontent in cases of clear breaches of international law.

3.2 Neutrality Concepts

The two main works on the concept of neutrality policy emerge from Suter (1998) and Riklin (1991). From the previous subsection, we recall the different definitions of neutrality, based on Suter (1998) and Widmer and Kreis (2007):

- Military non-alliance: no obligation or contract exists to support any belligerent power, yet the country may choose to support any side;
- Conflict-specific neutrality: a state declares its neutrality for a specific conflict. The nation should not be biased towards any of the belligerent powers and provide equivalent trade options for both sides. International treaties on the rights and duties of neutral nations are in place;
- Permanent neutrality: the declaration that a nation will not be biased towards any belligerent power, even before any conflict is foreseeable;
- Armed neutrality: the declaration of a nation that it is willing to defend its neutrality by its own means;
- Integral neutrality: a very strict and absolute interpretation of neutrality with isolationist aspects. No supranational organisations (e.g. EU, UN) should be joined, no economic sanctions should be followed;
- Differential neutrality: international organisations may be joined and economic sanctions may be followed if they are widely accepted by the international community. No military sanctions are followed. The aim to maintain unbiased towards any power is upheld;
- Active neutrality: a neutral nation's recognition of its responsibility for international peace and collaboration as a trustworthy third party. The neutral nation expresses its discontent in cases of clear breaches of international law.

Suter also defines three preconditions for the formation of Swiss neutrality: first, the absence of a consensus among the major powers due to their diverging geopolitical interests. Second, the absence of consensus within Switzerland on its foreign ties due to the diverging ethnical, cultural and cantonal interests. Third, Switzerland's status as a small state with little military threat potential. These preconditions can be broken down to the *balance of power*, *internal peacekeeping* and an *absence of threat* to the major powers.

We also note Suter's emphasis of the *requirement of self-defence*: Switzerland's borders were threatened only decades after 1815 by powers that had promised to guarantee them.

Finally, we note the precedence of *national security over neutrality policy*: neutrality policy is an important principle supporting Switzerland's security strategy: it aims at not being drawn into any conflict of foreign powers. When the country's national security is existentially threatened, a historic precedent for prioritising national security over neutrality has been set. Suter further underlines this claim by stating that the authors of the first constitution of the modern federal state did explicitly abstain from adding neutrality as one of the founding principles of the Swiss Confederation in 1848.

These principles exfiltrated from Suter's essay are consistent with Riklin's theory of *purposes* of neutrality. Riklin describes five purposes of Swiss neutrality, as shown in Figure 1. The purposes explain what major national or international interests require neutrality. The dimensions are the domains in which the relevance of these purposes are measured. The importance of a purpose might change over time, or is more or less relevant from a territorial (geopolitical) perspective, etc.

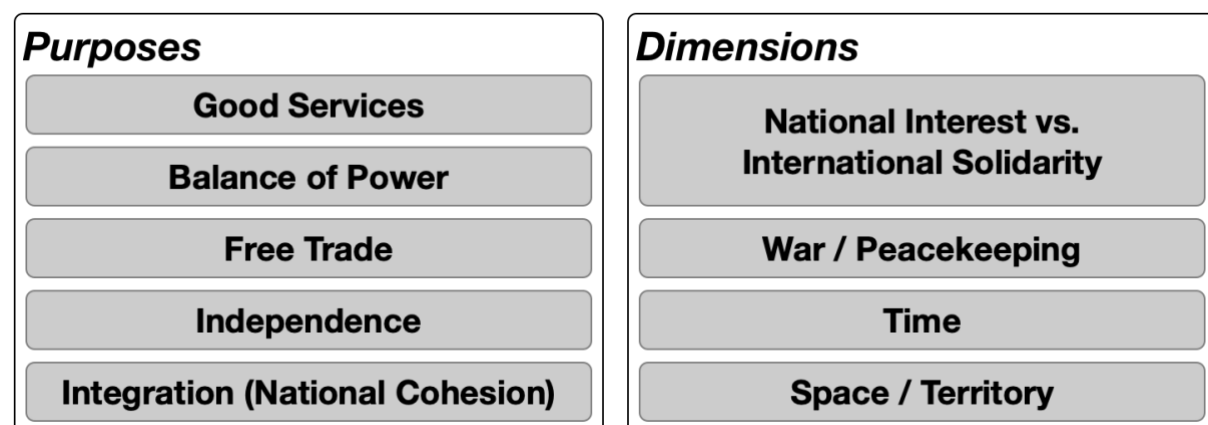


Figure 1: The functions and dimensions of state neutrality, according to Riklin (1991)

3.3 Current Implementation of Neutrality Policy

The current implementation of neutrality policy is based on a new implementation of differential neutrality with the addition of active neutrality. While it emphasises the aspect of international collaboration and the importance of providing good services to the international community, the other purposes remain relevant for Switzerland. Former diplomats underline the importance of a credible and trustworthy implementation of neutrality policy (Widmer et al, 2007) in order to maintain the option of active neutrality. Furthermore, they emphasise that, even though the geopolitical environment for Switzerland might seem peaceful in post-Cold War Europe, neutrality should still be upheld as basic principle of foreign policy in order to maintain independence and avoid foreign conflicts. Finally, neutrality enjoys very strong support in the Swiss population. Its acceptance rate is over 80%, sometimes even over 90% (Widmer et al, 2007). In the Swiss democratic system this means that an official breach of neutrality policy is politically infeasible.

4. Switzerland's Activities in Cyberspace

In order to understand the potential and limits of neutrality policy in cyberspace, we shortly outline the current state of governmental cyber activities in Switzerland. This section also covers examples of cyber incidents in government institutions.

4.1 Switzerland's Cyber Institutions and its Cyber Strategy

The main governmental organisation that analyses cyber incidents on a daily basis is *MELANI*. It monitors current cyber risks and major bugs and functions as an information hub between the private sector, critical national infrastructure providers, the intelligence service and also runs the government's CERT (*Computer Emergency Response Team*). Its competencies are limited to analyses, monitoring and distribution of information. A small unit connected with MELANI sits in the Swiss intelligence service in the Department of Defence. It is assumed that this unit might be capable of carrying out offensive actions.

Apart from the cybercrime prosecution unit of the federal police, the other main governmental cyber institution are the *Swiss Armed Forces*. Even though there has been a high amount of publicity on the introduction of a cyber unit, it is questionable what capability this unit has so far. The main recruiting scheme has only started in 2018, with approximately 18 recruits per semester (Swiss Armed Forces, 2018).

Switzerland has also released a National Cyber Strategy, meanwhile in its second iteration (Informatiksteuerorgan des Bundes ISB, 2018). The document outlines the responsibilities of MELANI and further government institutions with regard to incident management and protection of critical infrastructures. It also has a specific section on Cyber Defence. It does not go into depth and only covers main aspects. Nevertheless, active protection measures are a focus area for development of capabilities. Furthermore, a particular focus lies in the provisioning of intelligence information and the attribution of cyberattacks.

Noteworthy is also the section on international collaboration in cyber matters, where Switzerland aims at bringing together nations to generate a basic understanding of problems in cyberspace and potential resolution mechanisms.

4.2 Cyber Defence Case Examples

In recent years, several attacks on Swiss government institutions have been registered and publicly reported. Notable attacks are the series of data breaches at the Department of Foreign Affairs (Schweizerische Depeschenagentur, 2012), the RUAG case in 2016 (GovCERT.ch, 2016) and further attacks on the Department of Defence in 2017 (Der Bundesrat, 2017). The RUAG case is particularly interesting, as a detailed technical report is provided. It was not a direct attack on the Swiss Department of Defence. Rather, it attacked a governmentally owned defence contractor, RUAG, in order to gain access to confidential data shared with the contractor. The attack in 2017 is a follow-up on the 2016 attack, indicating that the initial attacker did presumably not get all the data intended from the attack in 2016.

The release of the technical report is particularly noteworthy, as it provides insights into how Switzerland responded to a significant foreign attack on one of its government institutions. A response is challenging. Conventionally, a military response to a military attack would be permitted for a neutral country. Self-defence, in particular a direct response to an attack, is always permitted. However, in cyberspace the authorship of an attack is easily blurred. States can plausibly deny that they authored an attack and so the attribution to an attack remains a matter of more or less substantial speculation. Hence, a direct response to a cyberattack by means of a counterattack is not a recommendable solution. The technical report released on the RUAG case provides an

interesting solution to this problem. The report was released publicly and provides a detailed technical analysis of the attack. Furthermore, it attributes the attack to a hacker group commonly associated with government activities of a specific country. Hence, the report publicly but indirectly blames a country for the attack. Furthermore, it provides a platform for Switzerland to present its technical capabilities with regards to attack analysis. The very detailed report bears an indirect message to any potential attackers: “beware, we know who is attacking us and we have the means to discover your attack!” Furthermore, it leaves room for speculation on the potential capabilities of Switzerland in the offensive domain, which might follow a cyberattack on Switzerland.

5. Future of Switzerland’s Neutrality Policy

We have discussed the current state of cyber studies, the history of neutrality policy and the current state of Switzerland’s cyber activities. The aim of the current section is to merge the findings of each previous section and to define the challenges they pose when brought together. We then outline potential solutions to the challenges.

5.1 Challenges

In Section 2, we discussed the problem of the scholarship gap regarding cyber studies in political science and the theory of revolutions disrupting the International System. Cyberspace has the potential of launching a first-order revolution, or *systems change*. Kello (2017) argues that cyberspace has already caused the International System to change, by significantly empowering non-state actors. This notion of a systems change is presumably the main challenge for the conventional implementation of neutrality policy. As we introduced in Section 3, the history of neutrality policy has evolved in an international system of sovereign states, i.e. the Conventional Model. While third- and second-order revolutions maintain this system—and examples of such revolutions have occurred over the last 200 years of history—, first-order revolutions impacts the way the International System works. Hence, some of the considerations on neutrality policy from Section 3 might not correspond to the current state of international relations anymore. Independence might have become a naïve wish in an interconnected world. Similar considerations are true for free trade in times of publicly fought trade wars. On the other hand, neutrality purposes, such as good services or the balance of power receive a new meaning: the emergence of non-state actors requires to also balance their power and to provide diplomatic or humanitarian services for them. It is questionable to which extent this might be accepted by states in the future.

Moreover, we have seen that the justification for neutrality has been made on the basis of geostrategic, i.e. territorial, considerations. In cyberspace, However, Switzerland has an indirect virtual border with any country, even if only indirectly. Hence, the basic environment for neutrality has become more complex.

A further aspect is the precedence of national security over neutrality. In the cyber age, where every component of a company or government can potentially be attacked, it becomes questionable whether neutrality is still maintainable. Is the cyber threat enough to cause an existential threat to national security? Or does neutrality, extended to cyberspace, offer additional safety and security from attacks? This matter requires careful evaluation and balancing of the potential of neutrality in cyberspace, its advantages, and the disadvantage in terms of cyber capability, cyber capacity and knowledge exchange, as this might have an impact on bias and trustworthiness.

Finally, we have outlined in Section 3 that an important precondition for neutrality is not only the choice of a country to be neutral but also a common interest of the international community—or at least a significant part of it—in favour of the neutrality of this country. It is unclear whether there is a general international interest for the case of a neutral country in cyberspace. An interest would require a benefit for the international community, which has yet to be elaborated.

We conclude that the main challenges are:

- the effect of the unprecedented systems change on neutrality policy;
- the impact of the previous point on the purposes of neutrality;
- the rupture of the geostrategic / territorial nature of a country’s security;
- the precedence of national security over neutrality policy in the cyber era;
- the benefit of neutrality in cyberspace for the global community.

5.2 Provisional Outline of Possibilities

Following the definition of challenges for neutrality in cyberspace, we would like to outline some potential solutions to these challenges relying on current developments in cyberspace.

First of all, the effects of the systems change have yet to manifest themselves in the International System. While there is an increased number of actors beyond state control in cyberspace, there is also an increased initiative of states to maintain the supremacy of states (i.e. the Conventional System). A prominent example is the UN Group of Governmental Experts (UN GGE), where Switzerland pushes strongly for a consensus-finding approach to answer challenges of cybersecurity (BAKOM, 2018). This approach is also described in the National Cyber Strategy of Switzerland (Informatiksteuerorgan des Bundes ISB, 2018). In case this approach fails, other actors apart from states will have true relevance, a process which has already started in the recent years. A typical example are the increased influence of large tech companies. Further examples are the emergence of hacker groups and their influence on global affairs. This increase of actors might increase the importance of neutrality policy: in terms of national security, neutrality might help avoid being targeted by the new global actors. Furthermore, the presence of a generally trustworthy mediator is beneficial for all parties.

The purposes of neutrality should remain unchanged by the systems change. However, their significance will be impacted; some purposes might increase in importance while others decline. As outlined previously, the significance of good services and balance of power could increase.

The rupture of the geostrategic and territorial nature of a country's security definitely has an impact on Switzerland's security. There is an increased interest in remaining neutral, as more virtual borders equal more potential attack origins and neutrality helps avoid potential conflict. Also, more virtual borders provide more potential partners for direct free trade. Hence, this challenge will presumably function as an accelerator for neutrality in the future.

The precedence of national security over neutrality policy is the most problematic challenge. The significance of the virtual weapon for national security is currently being discussed. An important aspect neutrality is the defence capability. Would a neutral country be able to accumulate sufficient knowledge and capabilities? Or is increased collaboration with foreign powers an indispensable asset for the defence strategy of small countries? We cannot answer these questions sufficiently for the time being.

When it comes to the benefit of neutrality policy for the international community, there are straightforward possibilities: A neutral country can ensure communication and diplomatic relations between parties who do not have any direct and official means of communication. Furthermore, a neutral country can provide analysis services of cyberattacks, as has been suggested by Mäder (2019). However, this can result in the country being targeted. On the other hand, the neutral country can gain important insights from the analysis work.

We conclude that a future of neutrality in cyberspace is possible. However, its detailed shape yet has to be defined. We can imagine a neutrality policy which takes into account the different nature of cyberspace by means of defining a *dual* neutrality policy: the conventional, stricter implementation for conventional conflicts, while applying a more flexible approach to neutrality in cyberspace, in order to allow more collaboration with other states for cyber capacity building. Furthermore, with the emergence of new actors in cyberspace, a very strict interpretation of neutrality policy in cyberspace is possible, in order to avoid being drawn into any conflicts. A particular interest also lies on the topic of the role of neutral countries for the global community.

6. Concluding Remarks and Future Work

We outlined challenges and potential solutions to neutrality policy in cyberspace. Further considerations are required in order to outline the borders of neutrality policy in the cyber era. In particular, the balance between national security and neutrality policy requires a more thorough analysis. As preliminary work, the neutrality purposes have to be freshly evaluated. The potential of a dual neutrality approach needs yet to be analysed. Finally, a study on the benefit of neutrality in cyberspace for the global community is necessary and a definition of the role of a cyber neutral country in an era of *global* conflict is required.

We would like to conclude by stating that the potential of neutral nations in cyberspace is high with regard to the system changing character of the virtual weapon, if a common ground for the benefit and requirement of cyber neutral nations can be found.

References

- Kello, L. (2017) *The Virtual Weapon and International Order*, Yale University Press, New Haven.
Nye, Jr., Joseph S. (2011) *The Future of Power*, PublicAffairs, New York.

The Hague Convention (1907) *Rights and Duties of Neutral Powers and Persons in War on Land*, The Hague, <https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0654.pdf>

The Hague Convention (1907) *Rights and Duties of Neutral Powers in Naval War*, The Hague, <https://www.loc.gov/law/help/us-treaties/bevans/m-ust000001-0723.pdf>

Suter, A. (1998) *Neutralität. Praxis, Prinzip und Geschichtsbewusstsein*, Eine kleine Geschichte der Schweiz, Suhrkamp, Berlin.

Riklin, A. (1991) „Funktionen der schweizerischen Neutralität“, *Passé pluriel. En hommage au professeur Roland Ruffieux*, Editions universitaires, Freiburg, pp 361–394.

Bonjour, E. (1946) *Geschichte der schweizerischen Neutralität. Drei Jahrhunderte eidgenössischer Aussenpolitik*, Helbing & Lichtenhahn, Basel.

Holenstein, A (2014) *Mitten in Europa: Verflechtung und Abgrenzung in der Schweizer Geschichte*, Hier und Jetzt, Baden.

Widmer, P. and Kreis, G. (2007) *Die Schweizer Neutralität: beibehalten, umgestalten oder doch abschaffen?*, Werd-Verlag, Zürich.

Swiss Armed Forces (2018) „Erste Erfahrungen mit dem Cyber-Lehrgang der Armee“, [online], Swiss Confederation, <https://www.vtg.admin.ch/de/armee.detail.news.html/vtg-internet/verwaltung/2018/18-09/erste-erfahrungen-mit-dem-cyber-lehrgang-der-armee.html>

Informatiksteuerorgan des Bundes ISB (2018) *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022*, Swiss Confederation, Bern.

Schweizerische Depeschenagentur (2012) „Bundesanwaltschaft untersucht erneuten Hacker-Angriff auf EDA“, [online], Tageswoche, <https://tageswoche.ch/allgemein/bundesanwaltschaft-untersucht-erneuten-hacker-angriff-auf-eda/>

GovCERT.ch (2016) *APT Case RUAG Technical Report*, Swiss Confederation, Bern.

Der Bundesrat (2017) „Cyberangriff auf die Bundesverwaltung entdeckt und Massnahmen ergriffen“, [online], Swiss Confederation, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-68135.html>

BAKOM (2018) „Engagement des Eidgenössischen Departements für auswärtige Angelegenheiten EDA im Bereich Cyber“, [online], BAKOM, <https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/strategie2018/faktenblaetter/FB%20EDA%20Cybersecurity.pdf.download.pdf/FB%20FAE%20Cybersecurity%20d.pdf>

Mäder, L. (2019) „Wenn der feindliche Zugang zum Computer gleich mitgeliefert wird“. [online], NZZ, <https://www.nzz.ch/schweiz/wenn-der-feindliche-zugang-zum-computer-gleich-mitgeliefert-wird-ld.1467220?mktcid=nled&mktcval=107&kid=2019-3-18>

Appendix B

Published Paper: *Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries*

The following paper [3] was accepted as a submission to the 2021 *International Conference on Cyber Warfare and Security* (ICCWS, ISSN: 2049-9870). It was presented at the conference in February 2021 and published in the conference's proceedings the same year.

Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries

Marcel Stolz

Centre for Technology and Global Affairs (CTGA) | Cyber Security Analytics Group

University of Oxford, UK

marcel.stolz@oriel.ox.ac.uk

DOI: 10.34190/IWS.21.082

Abstract: Intelligence agencies and defence forces usually work hand in hand in order to support the interests of a state. In cyberspace, however, their activities overlap and their goals may differ or even oppose one another. This paper outlines the potentially diverging interests of intelligence agencies and defence forces of the same state. The conceptualisation is supplemented by a case study of Switzerland's intelligence and defence organisation and a reflection on its particularities as a neutral country. The paper concludes by suggesting an organisational structure that avoids a conflict of interests between cybersecurity organisations of the same state.

Keywords: Switzerland, Neutrality, Cyberdefence, Cyberintelligence, Cybersecurity Dilemma, Cybersecurity, CNA, CND, CNO, CNE

1. Introduction

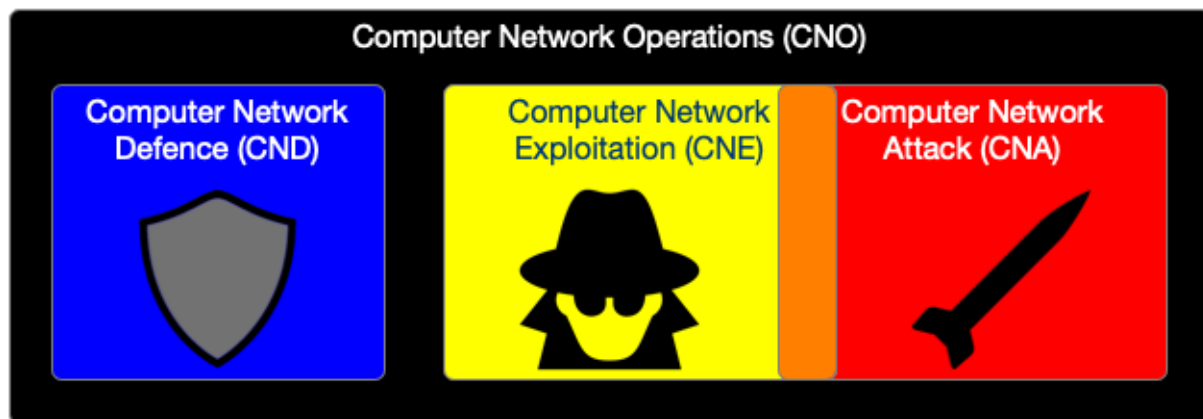
Traditionally, intelligence operations and defence measures are tools of security policy that work hand in hand in order to ensure the national interest in the realist perspective of the anarchic international system of states. In cyberspace, diverging interests can occur. In particular, different security actors of the same state may have conflicting interests when considering the deployment of specific technological assets ("cyberweapons" or malware). While entities that focus on defence might be more interested in a disrupting impact, intelligence entities traditionally focus on the exfiltration of information. Both intelligence agencies and defence forces might be drawing, knowingly or unknowingly, from the same or an overlapping set of technological assets. These technological assets may suffer in effectiveness or impact, depending on when or how they are deployed. This paper conceptualises and analyses this problem and provide a case study for the situation in Switzerland, a neutral country, in order to suggest an organisational structure that avoids conflicts of interest. The remainder of this paper is structured as follows:

A definition and clarification of terms are provided in Section 2. Thereafter, Section 3 introduces our conceptualisation of operations in cyberspace from the military and intelligence perspectives and Section 4 explains some of the problems when attempting to distinguish between military and intelligence operations in cyberspace. Section 5 outlines the problems that might occur from a state's perspective when its intelligence and military entities deploy assets independently and without further coordination. Section 6 follows with a case example of a cyberoperation against a Swiss state-owned defence contractor and Section 7 outlines the specific legal structures and units in Switzerland that define and deploy cyberoperations, respectively. Finally, Section 8 provides a structural recommendation for avoiding conflicts of interest and Section 9 draws some conclusions.

2. Terms

The following list provides a short nomenclature for terms used in this paper.

- *Security, intelligence, and defence / military entities.* The term 'security entity' is used for any agencies or organisations in a state that implement a state's security policy. Specifically, this includes intelligence and defence entities. Defence or military entities are those organisations that have a primary focus on defensive activities in a state, for example the armed forces. Defence entities are trained to achieve an impact in foreign or sometimes also home territory. This paper focuses on foreign territories and systems. Intelligence entities focus their activities on the exfiltration of information. They structure, analyse, and interpret this information in order to protect a state's security. While defence entities might contain organisational units that achieve an intelligence purpose (e.g., for reconnaissance and mission support), this paper focuses on their defensive nature. Intelligence activities might be considered to be of a passive nature, as their main aim is to retrieve information without being discovered by the opponent. Defence activities are of a more active nature, as their aim is to achieve a specific, often physical, impact. The term defence includes offence



activities in this paper, as 'defence' agencies also conduct offence activities but they are often referred to as defence measures.

- *Cyberdefence and cyberintelligence assets.* These terms refer to technical components that are used for operations in cyberspace, for example malware in the form such as worms, and viruses,. These assets are sometimes also referred to as cyberweapons.

Figure 1: The different types of CNO. CND is defined as non-intrusive. CNE and CNA are intrusive and overlap.

- *Adversary, opponent or opposing side:* This term is used for the party that is experiencing invasive operations in cyberspace, i.e., is victim to a cyberoperation.
- *Perpetrator or attacker.* This refers to the party that is carrying out an operation in cyberspace, known generically as the perpetrator.

3. Conceptualisation of Operations in Cyberspace

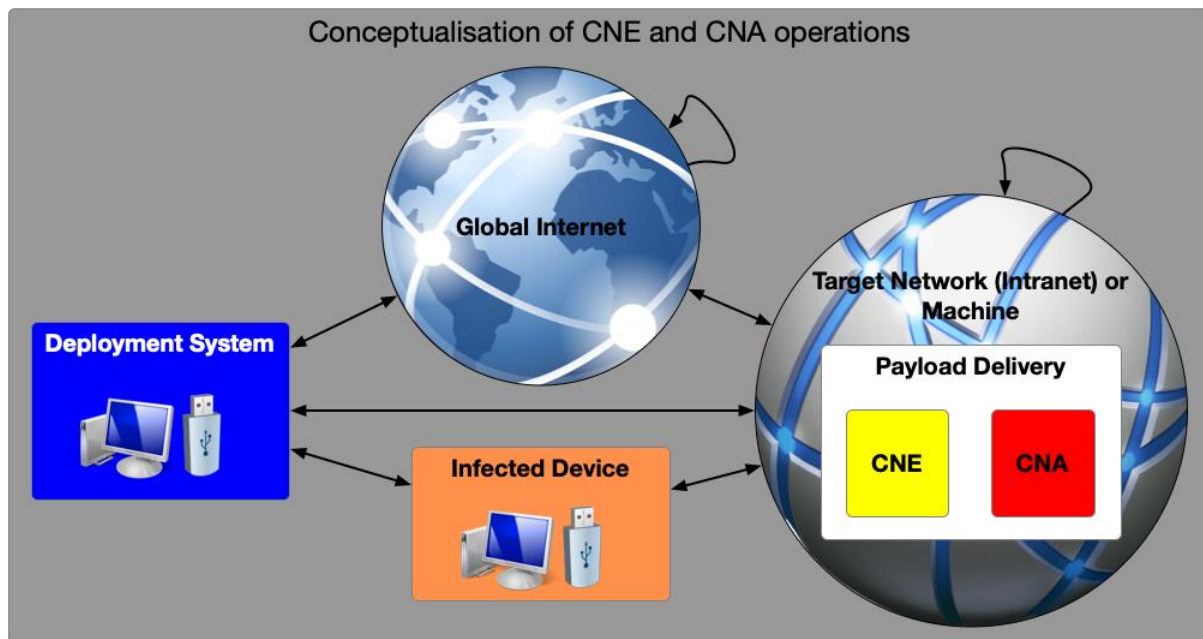
Operations in cyberspace usually involve the exploitation of security holes of computer systems and networks in order to achieve their goal. A technical, high-level conceptualisation of these operations in cyberspace is provided below.

Firstly, a concept common to many Western military organisations is introduced. It divides (state) operations in cyberspace into subcomponents. The overall term used for operations in cyberspace on a tactical level is *Computer Network Operations* (CNO). CNO are further divided into Computer Network Defence (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA), as illustrated in Figure 1. This division of CNO into CND, CNE, and CNA is common in NATO and some *Partnership for Peace* countries. For example, the Swiss Armed Forces, explain their understanding of these terms in their documents on military doctrine (Schweizer Armee, 2019). Similar definitions have also been outlined by Spring (2014) based on the *US Military Strategy for Cyberspace Operations* (US Department of Defence, 2006). Spring emphasises the disruptive component of CNA operations as well as their potential to destroy information in computers, networks, connected infrastructure. He further outlines that CNE focusses on the collection of information for intelligence or reconnaissance purposes and that CNEs do not alter the content or condition of a system; *"the infiltrated system appears the same as prior to a CNE"* (Spring, 2014, p. 234ff).

The focus of CND is to protect a party's own networks from attacks. For our purposes, CND does not include any intrusive measures or operations in external systems, machines, or networks. Excluding intrusive measures enables a clear distinction from CNE and CNA.

Both CNE and CNA affect external systems. An adversary might be interested in being able to distinguish these operations from one another in order to conduct appropriate military, intelligence, diplomatic, or other counter measures. CNE and CNA are conceptualised on the basis of their propagation through cyberspace and their effect on systems.

An illustration of CNE and CNA operations is shown in Figure 2. An operation is usually deployed from a system different to machines attributable to the perpetrator in order to ensure obfuscation. This is of particular interest for intelligence operations. Systems that deploy an operation might be USB sticks or computers that are attached to the global Internet. The most common approach is to deploy an operational asset via a deployment device on the Internet, i.e., the operational asset propagates through the Internet before reaching the adversary's network. This usually involves the arbitrary infection of intermediate devices that are not the main target, until the operational asset reaches its intended destination. A deployment system might also be specifically targeted with the knowledge that it will be connected to the adversary's network, or infect



machines that are not connected to the global Internet but will be connected to the adversary's internal network or its systems; as has been the case for Stuxnet (Buchanan, 2017). The illustration includes the possibility of propagation of an operational asset through the global Internet, by means of an intermediary device / system or possibly also by direct connection of the deployment system to the adversary's network or machines; these appear to be the most common options from a technological perspective. The propagation of the operational asset as it has been explained is applicable to both CNE and CNA.

Figure 2: Conceptualisation of intrusive operations in cyberspace.

The distinction of CNE and CNA is determined by means of the effect on the target system: CNE does not appear to alter the target system, while CNA has a (destructive) impact on the target system. This distinction is outlined in further detail in the upcoming section.

4. The (in-)Distinguishability of CNA and CNE

As illustrated in Figure 2, CNA and CNE are similar in terms of their propagation through cyberspace. Even as they reach their target system or network, they remain indistinguishable. Gaining access to a system or network by means of infiltration is common to both CNA and CNE. This does usually involve gaining control of a system. CNE and CNA differ only in terms of the payload delivery in the target system. Both exploit vulnerabilities to propagate and gain access to external systems. Once a CNE reaches its target, it applies a mechanism that allows access to sensitive information and its subsequent exfiltration. CNA, on the other hand, usually establishes a presence on the target system and afterwards delivers a (destructive) impact that will become recognisable to the opponent. However, CNA may gain access to a system or network and then remain idle for some time before the perpetrator decides to trigger the payload.

The opponent may, by means of CND, be able to identify operations aimed against it. Nevertheless, the opponent might not be able to identify whether the operation was a CNE or a CNA: as stated in the documents of the Swiss Armed Forces (Schweizer Armee, 2019), a CNE-like operation might function as reconnaissance in order to enable the later deployment of a CNA. The adversary could attempt to analyse the type of malware or infection used and the software it ports in order to try and identify the nature of the operation. However, this might induce significant delays in response to a discovered attack. A distinction between CNA and CNE operations is difficult for the adversary before any CNA payload is delivered and the impact discovered.

This indistinguishability of CNA and CNE operations can induce problems both for the adversary and the perpetrator. While the adversary will require a classification as either CNE or CNA in order to decide on adequate response measures, the perpetrator could be confronted with the accusation of having deployed a CNA operation while actually having deployed a CNE operation. As such, the indistinguishability could accelerate conflicts due to an alleged belligerent nature attributed to an operation. On the other hand, a conservative response by the adversary bears the risk of classifying an actual CNA operation as CNE and can result in a significant disadvantage for the adversary. This problem has been thoroughly analysed and

discussed by Buchanan (2017) and yields the *Cybersecurity Dilemma*, with a general tendency of accelerating conflicts in cyberspace and an advantage for the perpetrator.

One of the factors impacting the dilemma is the implicit consensus of the international community that (conventional) intelligence operations are generally accepted as “unavoidable evil” that all countries engage in. While this does not indicate that there might be no response to conventional or cyberintelligence operations, the response will usually not be of belligerent nature, as intelligence operations that are purely aimed at the exfiltration of information are not recognised as an act of war.

A further challenge has been outlined thoroughly by Egloff (2020): Even when a classification of an operation as CNA or CNE is possible, an appropriate response is only possible when the adversary is able to attribute the attack to a country or some other identifiable actor. As outlined by Egloff, states are able to attribute activities with some level of certainty. Nevertheless, publicising attributions and responding by means of diplomatic channels can pose a challenge, since final proof is often missing or cannot be disclosed.

Cybersecurity assets can be classified into two groups:

- Assets of the first group make use of commonly known vulnerabilities. In this case, these vulnerabilities are known to the global cybersecurity community. The perpetrator has to rely on potentially inappropriate CND measures.
- Assets of the second group make use of unknown vulnerabilities, so-called *zero-day* exploits. They form the second group of assets and are difficult to protect against or even discover. Knowledge of zero-day exploits is usually kept secret. Some of these zero-day exploits might be more suitable for CNA, while others might be more useful for CNE.

5. Differing Interests of Defence and Intelligence Entities

As outlined, military entities are typically interested in deploying CNA operations. They might also deploy CNE for reasons of reconnaissance. On the other hand, intelligence agencies are typically interested in collecting and analysing information in a covert manner and might use CNE operations for this purpose. Intelligence agencies do not generally deploy CNA operations, as this might be considered a belligerent act.

Hence, for intelligence entities it is essential that their CNE assets remain covert in nature: a discovery could provoke counter measures. While CNEs can be carried out by exploiting publicly known vulnerabilities, the chance of discovery by the adversary through CND is higher. In order to ensure that CNE operations remain undiscovered over longer time, intelligence entities will have a greater interest in deploying zero-day exploits and ensuring that these remain undiscovered.

Military entities share a similar interest when deploying their CNA assets during the reconnaissance phase of an operation. However, a reconnaissance phase might require less time than a typical intelligence operation. Discovery of the CNA is likely once the impact has been detected; it enables the adversary to search for malware, analyse the operation, and identify (unknown) vulnerabilities. Therefore, there is a high likelihood that zero-days in CNA will be discovered (or even made public). This increases the likelihood of discovery of any CNE operations that make use of the same zero-day exploits. Such a discovery might significantly impact the interests of the intelligence entity, as it puts ongoing information retrieval at risk.

This underlines the risk of defence and intelligence entities working against one another's interests in case they deploy the same zero-day exploits for their operations. In a country with many intelligence entities and a large military apparatus, such a scenario is highly likely.

6. Relevance for Neutral Countries and Case Study

Having outlined the theoretical background and conceptualisation of CNO, the specific practice in Switzerland is now analysed. Switzerland implements a policy of permanent neutrality and it faces additional challenges when transferring this policy from conventional geopolitics to cyberspace, as has been outlined by Stolz (2019). Since “*permanent neutrality is the rejection of war as an instrument of foreign policy*” (Spring, 2014), the deployment of CNA is only an option on the background of an evident and publicly credible case of self-defence. Nevertheless, a neutral country, as any other country, has an interest in deploying intelligence operations for information gathering. This poses problems when deploying CNE operations, since they might be misunderstood as CNA. Furthermore, a neutral country also faces challenges when falling victim to a CNA: the attribution problem stated earlier (Egloff, 2020) renders a definite identification of a perpetrator on the basis of publicly presentable proof difficult. A neutral country must develop mechanisms that allow some form of retaliation nevertheless.

The case of an attack on the government-owned defence company RUAG in 2014 (Swissinfo, 2014) reveals an interesting approach to this problem. Following the discovery of the attack in 2016, the Swiss government's computer emergency response team GovCERT.ch (now part of the *National Cyber Security Centre NCSC.ch* of Switzerland) released a report in May 2016 (GovCERT.ch, 2016). The report provides a detailed analysis of the malware deployed, the timeline of the operation, and it documents the malware's similarity with other malware attributed to specific hacker groups allegedly close to a specific state. While the report does not explicitly attribute the attack to that state, it implicitly outlines the plausible connection. The spokesman of the Swiss Attorney General stated on the case that: *"only state actors can be taken into account."* (swissinfo.ch, 2016).

The publication of the report allows to implicitly induce public blame to the plausible authors of the attack, while avoiding an explicit (diplomatic) confrontation or retaliation. Furthermore, the report signals the defence and analysis capabilities of Switzerland. Both implicit blame and signalling of capabilities can be considered to have some deterrent effect on potential perpetrators. Moreover, the publication of a technical analysis yields any vulnerabilities exploited and malware used less applicable for future operations. The disclosure of the technical details of the attack enables others to discover operations carried out with the same malware or exploiting the same vulnerabilities. In case the same operation is or has been experienced by a non-neutral state, the implicit attribution to a state or state-controlled actor might even yield a counter-operation (potentially a CNA) against the plausible author of the operation, which can be considered to act as a further deterrent feature of publicising the report.

The report also illustrates an important point outlined earlier: CNE operations aim at exfiltrating information over a longer period of time. The RUAG case started in 2014 or earlier and was only discovered in 2016. Once the operation was discovered by the opponent, appropriate defensive action was taken swiftly in order to avoid any further exfiltration: The detailed analysis report was published in May 2016, meaning that the respective malware was made public within only five months of discovery. It may be assumed that technical details had already been shared significantly earlier with relevant parties (e.g., befriended services or critical national infrastructure providers). Would a CNA using the same assets have been deployed before the discovery date of the RUAG case in 2016, it would presumably have led to an earlier discovery in the case experienced by RUAG.

The report also shows that once access was gained to the network of RUAG, machines on the network of RUAG were under control of the perpetrator. While these machines were only used for the purpose of data access and exfiltration, they were on an internal network of RUAG that was not directly connected to the Internet. Access to this internal network could have also been used in a later step to induce destructive activity that would have needed to be considered CNA rather than CNE.

The RUAG case illustrates how a CNE (or even a CNA) can be responded to by a neutral or peace-seeking country.

7. Structural examples in Switzerland

It has been explained how CNE and CNA can be responded to in a de-escalatory manner and with a deterrent effect, the structures that can lead to potentially diverging interests of military and intelligence entities require further analysis. These structures are outlined in the following based on the example of Switzerland.

Switzerland restricts any measures of CNE and CNA to a strict regime of control under its intelligence and military law. Military or intelligence entities are the only actors in Switzerland that are legally entitled to execute CNE and CNA operations and may do so only when certain conditions are met.

Article 100.1 of the Swiss Military Law (Federal Assembly of the Swiss Confederation, 1995) covers military security, i.e. the protection of the infrastructure of the Armed forces. *Lit. c* states that the Armed forces may *"in the case of an attack against military network and information systems take the required measures"* and *"[the armed forces] may infiltrate computer systems and computer networks that have been used for such an attack, in order to disturb, prevent, or decelerate the access to information; these measures require, except during times of declared engagement in national defence, the approval of [the Swiss government,] the Federal Council"*. While this article permits the deployment of CNA and CNE operations, these activities require explicit governmental permission or are restricted to times of active engagement in defensive missions. They are further limited to the case of a direct response to a discovered CNE or CNA operation. Furthermore, *lit. e* implicitly allows the deployment of CNE operations: *"[The armed forces take] preventive measures [against espionage, sabotage, and illegal activities] and obtain the necessary information if: 1. The armed forces are engaged in peace support or national defence missions; 2. The armed forces are engaged in internal support missions and the [CNE] measures are explicitly permitted"*. This implicitly restricts the armed forces to CNE

operations in peace time and only permits the deployment of CNE operations when certain conditions are met. Since Switzerland has constantly deployed armed forces in peace support missions over the last decades, CNE can be considered standard practice within the armed forces. However, it is noteworthy that the deployment of CNA operations is restricted to times of declared engagement of the armed forces in national defence missions or requires explicit permission from the Swiss government.

The intelligence law of Switzerland has been revised in 2016 and was subsequently approved by means of a popular vote (Swiss Department of Defence, 2020). The intelligence law regulates and restricts the deployment of CNA and CNE operations by the intelligence service (Federal Assembly of the Swiss Confederation, 2020). *Article 26.1* defines in *lit. d* the requirement of explicit approval for “*the intrusion into computer systems and networks in order to: 1. collect information present in these systems or transmitted from those systems; 2. disturb, prevent, or decelerate the access to information in case these computer systems and computer networks are used for attacks on critical infrastructure*”. This applies equally to activities on networks and systems based in Switzerland as well as abroad. Furthermore, *Article 37* defines that if “*computer systems or computer networks abroad are used for attacks on critical national infrastructure, the Federal Council [(national government)] decides on the implementation of [CNA] measures [abroad]*”, and that “*The intelligence service may infiltrate computer systems and computer networks abroad in order to acquire information [...] about activities abroad [...] The head of the DDPS [Department of Defence], after consultation with the head of the FDFA [Department of Foreign Affairs] and head of FDJP [Department of Justice and Police], decides on the implementation of [CNE] measures*”. Hence, any CNE or CNA operation carried out by the intelligence service abroad requires explicit approval by a number of ministers or a majority of the government ministers, respectively. Furthermore, CNA may only be conducted by the intelligence service in the case of attacks against critical national infrastructure.

The sole two entities in Switzerland that are entitled to carry out both CNA and CNE operations are, therefore, generally restricted to CNE during peace times. Only very specific circumstances, such as a declared case of national defence, a (cyber) attack against military information systems, or a (cyber) attack against critical national infrastructure, permit deployment of CNA operations and require additional approval on the ministerial level. It is noteworthy that the armed forces are restricted to cases of self-defence (i.e., to protect their own infrastructure). The intelligence service, on the other hand, may deploy CNA operations in order to protect critical infrastructure providers. This presumably minimises the risk of CNA operations being understood as a belligerent act; a deployment of CNA operations by the armed forces would suggest a belligerent character.

The armed forces may further only engage in CNE operations required for the support of peace missions. The intelligence service may engage in further CNE operations in order to acquire information in the national interest but requires ministerial approval for the deployment of any such operations. As has already been stated, Switzerland’s “*permanent neutrality is the rejection of war as an instrument of foreign policy*” (Spring, 2014). Therefore, the engagement of Switzerland in CNA operations appears to be a purely reactive scenario to clearly specified cases aimed at harming the national interests of Switzerland. With regard to the Cybersecurity Dilemma, as outlined by Buchanan (2017), this clear signalling contributes to a state of stability and predictability, since Switzerland is not known for measures of “active defence” or “preemptive measures” in the international community and is generally considered a state that strictly complies with its own laws. Therefore, countries do not have to fear CNA operations emerging from any entities in Switzerland unless a clear case of a (cyber) attack against critical infrastructure has been discovered by the Swiss authorities.

While the regulations for the deployment of CNE operations are less restrictive, a country experiencing CNE operations from Switzerland does not have to anticipate these measures being of a potentially belligerent nature, unless the very clear criteria that can trigger a CNA response are met. This has a potentially deterrent effect, while contributing to stability and predictability by means of the careful restriction of CNA to specific cases. The current law seems to indicate that deployed CNE operations are primarily used for intelligence purposes. The engagement in intelligence activities, which are tolerated by the global community as necessary although undesirable, could bear the risk of being interpreted as reconnaissance in preparation for CNA operations. Due to the strict restriction of CNA operations to very specific cases, however, an entity experiencing CNE that could be used for reconnaissance does not have to interpret this CNE as potentially threatening or belligerent act unless it decides to engage in CNA against Switzerland itself.

Having analysed the legal foundation specific to Switzerland’s application of CNE and CNA, the organisational specifics are discussed in the following. The intelligence service and the armed forces are separate entities within the organisational structure of the Swiss Department of Defence (DDPS). Since both of these administrative units may deploy CNE and CNA operations, it requires consideration whether this also means that the technical capabilities with regard to CNE and CNA are separate, i.e. exist within both units. The

division-level *Armed Forces Command Support Organisation* (AFCSO) includes the unit designated for the technical preparation and deployment of cyberoperations: on its website (Swiss Confederation–Swiss Armed Forces, 2020), AFCSO states that the *Centre for Electronic Operations* “is responsible for the defence against attacks from cyberspace, electronic warfare and cryptology”. Furthermore, it is “in charge of radio and cable communications intelligence. It provides the DDPS’s intelligence services with information and carries out electronic operations in cyberspace and electromagnetic space”. The *Intelligence Service Ordinance* further confirms this by stating in *Article 26* that the specific technical tasks for the intelligence service are carried out by the Centre for Electronic Operations (Federal Council of the Swiss Confederation, 2017). While any detailed documentation on the distribution of responsibility is likely classified, there is plausible reason to assume that the responsibility for preparing and carrying out CNE and CNA operations is generally delegated to the Centre for Electronic Operations, both for the intelligence service and the armed forces. Nevertheless, this does not guarantee different interests of defence and intelligence entities are well-balanced: The Centre for Electronic Operations is part of the armed forces by virtue of being incorporated into the Armed Forces Command Support Organisation; it provides services to the intelligence service while being incorporated into the military part of the Swiss Department of Defence. Hence, military interests could take precedence. Assets with a high likelihood of success might be withheld for future CNA operations.

Generally, a specific asset might have characteristics that are of higher value for some applications while being less relevant but still useful for other applications. These characteristics should be considered when deciding on the use of specific assets for their deployment in CNA or CNE operations. While the consolidation of technical capabilities for CNE and CNA within one central entity is a reasonable organisational step in order to prevent a divergence of interests, it is not a guarantee for an optimal deployment of zero-day capabilities.

8. Recommendation for Avoiding Conflict of Interests

A conceptualisation and differentiation of cyberoperations from an intelligence and military perspective, and the potential conflicts of interest have been discussed in the previous sections. Furthermore, a case study on the doctrinal, legal, and structural situation in Switzerland has been introduced and the case of an attack on the Swiss defence contractor RUAG has been discussed. The aim of this section is to recommend structures that enable a state to avoid the potential conflict of interests outlined.

A central unit responsible for the technical capability in the domain of CNE and CNA, such as Switzerland’s Centre for Electronic Operations, can support a balancing of defence and intelligence interests. This paper suggests this central unit should be defined as the sole organisational unit responsible for the development and deployment of CNE and CNA assets. It is believed that this prevents zero-day exploits and other assets being deployed without sufficient care or coordination. In order to enable a balanced decision, this central unit should further maintain a storage system for the cybersecurity assets it develops. It should also classify the assets according to predefined characteristics, which should reflect the requirements of defence and intelligence operations as well as the interests of the respective entities. These responsibilities are depicted in Figure 3 on the left-hand side as part of the *Technical Unit*. In the middle of Figure 3, the responsibility of balancing interests and deciding on which assets to deploy to a separate *Decision Unit* is displayed. The Technical Unit and the Decision may be merged into the same unit. They are represented as separate units in order to emphasise that technical concerns and decision concerns can be separated. This might be useful in case the Technical Unit is incorporated into the structure of either the military entity or the intelligence entity, as has been explained for the case of the Swiss Centre for Electronic Operations. The decision base for the Decision Unit should be provided by means of a classification and storage system of the assets developed or gathered by the Technical Unit. It is important that the Decision Unit collaborates with the Technical Unit on the definition of relevant characteristics, which is indicated by means of the arrow connecting the respective boxes in Figure 3.

Figure 3 further depicts the role of an intelligence or military / defence entity on the right-hand side. It is suggested that in case a security entity would like to deploy an intrusive cybersecurity operation, i.e., a CNE or CNA operation, it should provide a detailed technical request to the Decision Entity. Such a request might contain technical requirements and details on the systems and networks that need to be infiltrated, the potential impact of a CNA operation, the urgency and importance of a request, etc. The Decision Unit may then process the request by means of consulting the stored cybersecurity assets that have been developed by the Technical Unit. It might find that an appropriate asset is present and should be deployed. It might also find that the low urgency or minor importance of an operation request does not justify the deployment of a highly valuable and effective cybersecurity asset (e.g., a zero-day exploit) and decide that the request should be served by means of deploying a less valuable and potentially less effective cybersecurity assets. It might also decide that an asset should not be used in order to not compromise another operation that has already made use of the same asset, or it might decide that a suitable asset needs yet to be developed etc.

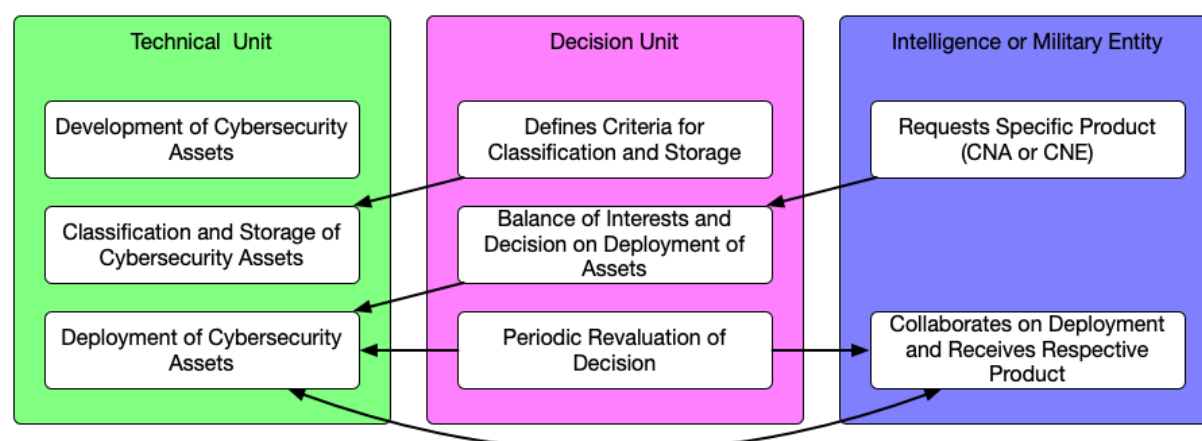
The Decision Unit ensures that the available assets are deployed in the most effective way and without compromising the interests of other operations. Finally, the security entity's request is forwarded from the Decision Unit to the Technical Unit. The Technical Unit deploys the respective assets and conducts the operation in collaboration with the security entity that has requested the operation. It delivers related products or reports to the requesting security entity. It might also be useful for the Decision Unit to periodically review ongoing operations, in case they are deployed over a longer period of time. This aspect is

Figure 3: Suggestion for the division of responsibilities between organisationally separate units / entities. included in Figure 3.

The structure outlined resolves the problem of differing interests and potentially mutually harmful operations. It does not, however, resolve the underlying problem of the Cybersecurity Dilemma: CNE and CNA operations are difficult to distinguish unless the destructive impact of a CNA operation has already been deployed and is recognised by the adversary. Nevertheless, the use of a storage and classification system allows for a detailed internal documentation of the use of and reason for deployment of CNE or CNA operations. Such an internal documentation could be further enhanced and retrospectively made semi-public (similar to classified archives), in order to support the plausibility of claims by the perpetrator about CNE operations not having a belligerent character. An enhanced documentation mechanism might also be useful in order to defend a CNE operation in case of a potential legal dispute in international courts.

9. Conclusion

Potential conflicts of interests of intelligence and defence entities when deploying the same or similar cybersecurity assets have been identified in this paper. The relevance of this theoretical discussion has further been underlined by a case study on Switzerland: The analysis of the RUAG report supports the relevance of our theoretical claims. Furthermore, it has been explained how the RUAG case serves as an example of both a de-escalatory and deterrent response to an operation. The usefulness of this response for the Swiss foreign policy principle of permanent neutrality has been emphasised; this might also be relevant for non-neutral countries as a peaceful and deterrent response. Moreover, CNE and CNA operations in Switzerland have been explored by analysing their legal boundaries. On the background of the Cybersecurity Dilemma and our conceptualisation, it has been concluded that the restrictive legislation on deployment of CNE and CNA operations has a de-escalatory effect while ensuring that the national interest can be met. This is surprising, as



it might seem contrary to the escalatory intuition (“offence advantage”) the Cybersecurity Dilemma suggests. Subsequently, the structures present in Switzerland’s administration for CNE and CNA operations have been discussed. It has been concluded that the centralised structures reduce a potential conflict of interests between intelligence and defence entities. The usefulness of further organisational measures has been explained. Finally, this paper suggested an organisational structure that addresses the conflict of interests outlined and builds on some of the structures identified as useful in the Switzerland case study.

While the suggested structure is sound in theory, its effectivity would need to be further analysed in practice and this is suggested as point for further research. Furthermore, the de-escalatory measures outlined on the basis of both the RUAG report and the strict legal boundaries in national legislation deserve more thorough consideration as policy option for the global community. They might complement the suggested structural implementation for CNE and CNA operations in order to ensure a national cyberpolicy aimed at de-escalation and minimal friction.

References

- Buchanan, B. (2017) *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. doi: 10.1093/acprof:oso/9780190665012.001.0001.
- Bundesminister des Innern (2016) ‘Cyber-Sicherheitsstrategie für Deutschland 2016’, (09.11.2016), p. 25. Available at: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (Accessed: 4 May 2017).
- Egloff, F. J. (2020) ‘Contested public attributions of cyber incidents and the role of academia’, *Contemporary Security Policy*. Routledge, 41(1), pp. 55–81. doi: 10.1080/13523260.2019.1677324.
- Federal Assembly of the Swiss Confederation (1995). *Bundesgesetz über die Armee und die Militärverwaltung* (510.10), retrieved from: <https://www.admin.ch/opc/de/classified-compilation/19950010/index.html>
- Federal Assembly of the Swiss Confederation (2020) Bundesgesetz über den Nachrichtendienst (NDG). Bern. Available at: <https://www.admin.ch/opc/de/classified-compilation/20120872/index.html>.
- Federal Council of the Swiss Confederation (2017) Verordnung vom 16. August 2017 über den Nachrichtendienst (Nachrichtendienstverordnung, NDV). Available at:
- GovCERT.ch (2016) ‘APT Case RUAG Technical Report’, (2016-05–23), p. 34. doi: 10.1089/lap.2006.05083. <https://www.admin.ch/opc/de/classified-compilation/20162430/index.html> (Accessed: 30 November 2020).
- Schweizer Armee (2019) *Taktische Führung 17 Kapitel 7 – Verteidigung*.
- Spring, A. (2014) *The international law concept of neutrality in the 21st century. An analysis of contemporary neutrality with a focus on Switzerland*. Edited by T. Cottier et al. Zürich / St. Gallen: Dike.
- Stolz, M. (2019) ‘On Neutrality and Cyber Defence’, in Cruz, T. and Simoes, P. (eds) *18th European Conference on Cyber Warfare and Security*. Coimbra: ACPI, UK, pp. 484–491.
- Swiss Confederation–Swiss Armed Forces (2020) Armed Forces Command Support Organisation AFCSO. Available at: <https://www.vtg.admin.ch/en/organisation/afcso.html> (Accessed: 30 November 2020).
- Swiss Department of Defence, Civil Protection, and S. (2020) Das neue Nachrichtendienstgesetz der Schweiz. Available at: <https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/nachrichtendienstgesetz.html> (Accessed: 16 November 2020).
- swissinfo (2018) *Swiss close investigation into cyber attack on defence firm - SWI swissinfo.ch*. Available at: https://www.swissinfo.ch/eng/ruag_swiss-close-investigation-into-cyber-attack-on-defence-firm/44352550 (Accessed: 16 November 2020).
- US Department of Defense (2006). *The National Military Strategy for Cyberspace Operations*. Washington D. C. Available at: <http://www.bits.de/NRANEU/others/strategy/07-F-2105doc1.pdf>.

Appendix C

Published Paper: *Platform Neutrality*

The following paper [164] was accepted as a submission to the 2021 *International Conference on Cyber Warfare and Security* (ICCWS, ISSN: 2049-9870). It was presented at the conference in February 2021 and published in the conference's proceedings.

Platform Neutrality—A Solution for the Social Media War?

Marcel Stolz

Centre for Technology and Global Affairs (CTGA) | Cyber Security Analytics Group

University of Oxford, United Kingdom

marcel.stolz@oriel.ox.ac.uk

DOI: 10.34190/IWS.21.081

Abstract: Neutrality is a concept applied by states during times of war. The example of Swiss Neutrality has been most prominent among states, implementing a concept that also allows long-lasting neutrality practice during times of peace.

While the future of state neutrality in cyberspace remains open, its example provides inspiration for the ongoing development of the relationship between social media platforms (or large technology companies in general) and the state. This paper contextualises the work on platform neutrality on the background of state neutrality and explores its suitability for large technology companies. Furthermore, this paper outlines how concepts from state neutrality can be applied for technology companies operating in a global context and reflects on the benefit of such principles based on most recent developments in social media self-regulation during the coronavirus pandemic, the *Black Lives Matter* movement, and the US elections.

Keywords: Platform Neutrality, Social Media, Facebook, Twitter, State Neutrality, Fifth Estate, International Relations Theory, Coronavirus, Misinformation, Freedom of Speech, Digital Human Rights, Online Censorship

1. Introduction

The global importance of social media and technology platforms has become more apparent than ever during the year 2020. On three occasions social media platforms, such as Facebook and Twitter, played their part in managing information and serving as a discussion forum of discussion: first, the emergence of the Coronavirus pandemic has become a major element of discussion throughout 2020. Second, the *Black Lives Matter* movement has led to a broad and global discussion about racism and inclusion, which has also been led through platforms such as Facebook and Twitter. Finally, the elections in the US in November 2020 have received significant attention on social media platforms, including the claims of election fraud following the election.

In particular during times of “*lockdown*”, such platforms have become tremendously important as a means for accessing news, communicating with governmental and other institutions and for political discussion. These platforms have been described as the *fifth estate* of power in liberal democracies (Dutton 2020). Due to negative experiences with “hate speech” and misleading or contradicting information, requests for censorship or stricter control of online platforms have arisen. However, the nature of cyberspace is inherently global and challenging for regulation. Affected companies are subject to a specific jurisdiction—in many cases the US—but provide services globally. The inherent value of these platforms is that they are available globally and that they virtually bring together users and customers from different countries. Users share content, generate and consume information, and participate in discussions or use other services offered by the platform providers. Content is generated by platform “participants”. Creating a strict regime of regulation with many restrictions carried out on a national level would breach the global character that makes these platforms unique. Some approaches have been made to overcome clear cases of criminal activities, since these usually share the consensus and thus support of a sufficient number of countries. However, regulating content globally beyond such clear cases is a major challenge. Platforms such as Facebook or Twitter have initiated a regime of self-regulation, in order to address some problems. These platforms offer a forum for global discussion with impact on national politics and democratic procedures; how should these platforms relate to the state and how should they be controlled while ensuring their global character is not nationally compartmentalised? It has been argued that these platforms should be considered an additional actor in the realist global system of states of international relations (Kello, 2017).

This paper outlines an approach towards the relation between states, as the main actors of the international community, and globally operating social media platforms, such as Facebook and Twitter. It introduces the novel concept of *platform neutrality*, which extends the current economically-focussed definition of the term. The concept of platform neutrality is set into relation to state neutrality, in order to provide a historic foundation on a similar concept for states.

The remainder of this paper is structured as follows: Section 2 introduces the concept of state neutrality. Thereafter, the current economically focussed definition of the term platform neutrality is outlined in Section

3. Section 4 analyses some cases of developments on social media platforms during 2020 and how social media platforms have responded to them. Finally, Section 5 introduces the conceptualisation of platform neutrality and Section 6 draws conclusions and reflects on future work.

2. An Inspiration: State Neutrality

State neutrality is a concept known in conventional international politics. Its historic tradition and potential for cyberspace has been discussed by Stolz (2019) and the respective conceptualisation is shown in Figure 1. The most prominent example of a permanently neutral country is Switzerland. Relative neutrality is defined in international law (Spring, 2019) and its main aim is to ensure the rights and duties of neutral countries with respect to specific conflicts, in order to ensure that third parties are not drawn into a conflict. Permanent neutrality, however, extends beyond the definition of relative neutrality in international law. It relates to a concept of permanent non-alliance and neutrality towards any potential future conflict.

The functions in Figure 1 show additional functions of permanent neutrality. While remaining independent from a third-party conflict might be the initial motivation for a policy of permanent neutrality, a permanently neutral country also needs to ensure that the global community has an interest in its neutrality. This ensures the neutral status is respected and defended by a global consensus. The bottom three functions in Figure 1 determine benefits for a neutral country, while the top two functions determine the external benefits.

Integration enables a country to maintain its internal cohesion. External conflicts might lead different groups within a country to work against one another, potentially destabilising it. Neutrality ensures that the effects remain limited. *Independence* refers to a country's ability to act independently from pressures present in alliances or other international interest groups that might restrict the future scope of action. The aspect of *free trade* is related to independence; it has an economic focus. The external party's interest in a country's neutrality policy is reflected by the function of a *balance of power*. Foreign powers may have an interest in some territory (or institution) remaining neutral in support of a balance of power, for example due to a country's geopolitical location that would upset this balance if the country became part of a specific block. *Good services*, finally, states that a neutral country should provide services it can provide credibly only due to its neutrality; it may provide a forum or act as a mediator for other countries, for example.

These factors may be essential for the consideration of the future role of global social media platforms and the companies that run them. While the specific factors might differ in the case of globally operating Internet platforms, the underlying motivations serve as an important inspiration for the concept of platform neutrality. The dimensions that are affected by the functions may differ from those of states: social media platforms, for example, have a limited impact on territorial aspects in a conventional sense. Time will also be relevant for platform neutrality, in the sense that their neutrality also has to be based on a long-termed, or permanent, foundation. While the terms of war or peace might be less applicable for social media platforms, a similar dimension of societal tensions or political disputes might be relevant for platform neutrality. A social media platform provider will also need to balance their own interests to the general interest of the global community. This does not only refer to the interests of states but also global principles of human rights or protection of individuals ("civilians").

3. Current Approaches to the Term of Platform Neutrality

Section 1 outlined the growing importance of social media platforms based on work by Dutton (2020) and Kello (2017). Section 2 explained the concept of state neutrality. The idea of technological neutrality is not

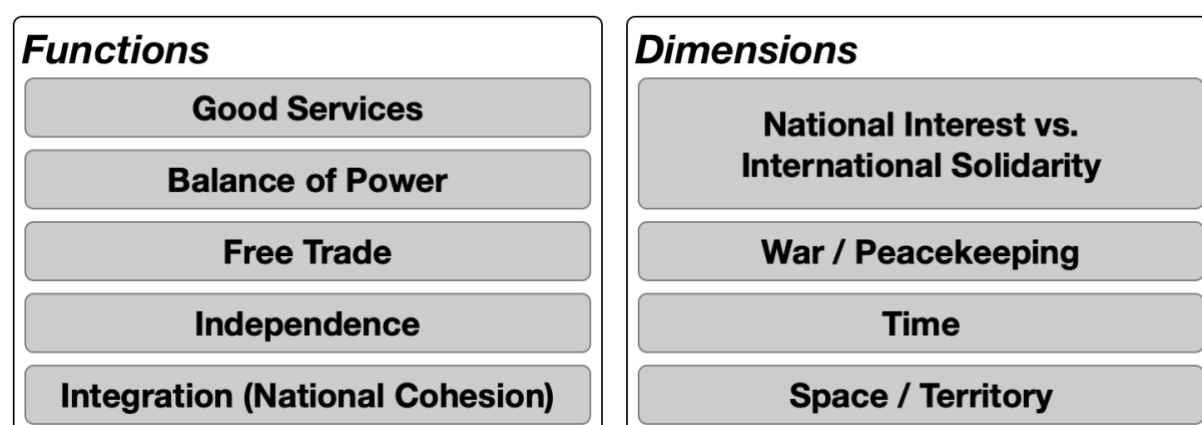


Figure 1: Functions and Dimensions of State Neutrality (Stolz, 2019).

new. The term of net neutrality has been introduced by Wu (2003) with a particular focus on the neutrality of Internet Service Providers (ISPs), in relation to the Internet traffic they route for users and content providers. Net neutrality bears an economic focus; ISPs should not favour traffic by specific content providers at the cost of other content providers and their users, in order to enable a free market of content. Furthermore, they should not restrict the use of their networks to specific application layer protocols, such as http(s) (for web browsers), streaming protocols (for services such as Netflix), etc. Rather, they should allow broad use of the Internet for all sorts of applications layer protocols.

Platform neutrality has also been discussed under an economical focus (Conseil National Numérique, 2014): Platform Service Providers (PSPs), such as Google, Facebook, or Twitter, should remain economically neutral towards services they provide. Originally, some PSPs built services and subsequently favoured their own appliances running on these services, generating a distortion of free market rules.

Gao and Yang (2015) relate the term of platform neutrality to net neutrality. Krämer and Schnurr (2018) specifically focus on how the EU should regulate the economic neutrality of PSPs. The latter argue that economic platform neutrality should not be regulated by imposing conditions of neutrality but rather by means of greater transparency in order to ensure a fair free market.

The introduced concepts in the literature of net and platform neutrality both argue with fairness of the free market and effectivity of the services offered. While this focus on economic fairness ensures a prosperous development of markets, it neglects an important aspect that is imminent to the social nature of platform services: the platforms provide a global forum for users and institutions. Not only should the access to services (such as advertisements) be fair for customers and users; the forum that allows discussion and promotion of opinions should be fair for all users. Such a call for fairness for the global forum provided by PSPs is underlined by claims that PSPs offer what is part of the *fifth estate* of liberal democracy (Dutton, 2020) and are a new non-state actor that has to be considered in addition to the international system of states of global conflict and cooperation (Kello, 2017).

4. Social Media Platform Developments during 2020

As outlined, political and social aspects have barely been considered under the term *platform neutrality*. This section discusses three cases arisen in 2020 that have further substantiated the underlying problems of regulation of global platforms. This is of particular relevance for liberal democracies, which rely on the ancient idea of a forum for free discussion. While such fora are conventionally controlled by means of national laws and enforced by the state, the global nature of online platforms introduces problems.

4.1 Misinformation during the Coronavirus Pandemic

The emergence of the Coronavirus pandemic has led to “lockdowns” in Europe and the US from March 2020 onwards. These lockdowns have led to an increase of people working from home and therefore also relying more on online platforms for work and social interaction. Social media platforms have received increased attention as a consequence due to online discussions on topics connected with the pandemic. The spread of false information through Facebook has been subsequently declared a “*major threat to public health*” (AVAAZ, 2020). Sites spreading misinformation have been found to receive four times more attention than the information spread by trustworthy sources, such as the *World Health Organisation* (WHO) (Stauffacher, 2020), and Facebook’s algorithms have been found to favour misinformation. While Facebook has claimed to take action by means of warnings attached to potential misinformation campaigns, this has been found to be ineffective as it only flagged 16% of misinformation (Stauffacher, 2020). This was contradictory to attempts of Facebook and other social media platforms of marketing themselves as supporters for tackling the global pandemic earlier in the year (Stauffacher, 2020b). It has been pointed out, however, that the distinction between misinformation handling and censorship is delicate (Stauffacher, 2020b), and indeed PSPs have been criticised to restrict freedom of speech in an illegitimate way, even if this happened accidentally. For example, Twitter had blocked links to the Swiss website *corona-data.ch*, even though the website’s contents were legitimate and trustworthy. Such unintended consequences fuelled conspiracy theories about the pandemic. Further efforts by social media companies included the launch of information centres that should provide unbiased facts (Hatmaker, 2020). Furthermore, a ban on specific ads, e.g., facemasks, was announced. Due to problematic posts and statements from politicians, social media platforms further started removing posts of publicly elected representatives, such as the Brazilian president Jair Bolsonaro (Their, 2020). This first ever deletion of posts on the basis of misinformation was an important precedent. Later in the year, a similar precedent occurred with the first ever deletion of a post by the US president, Donald Trump, also in

connection with a post classified as misinformation (Kormann, 2020). Facebook justified deletions by stating that they spread misinformation and infringed the platform's guidelines. Youtube also took steps in connection with the pandemic to avoid the spread of misinformation: it introduced fact-check panels under videos relating to specific search terms (Vincent, 2020). Twitter took a more radical approach by deleting accounts that spread conspiracy theories (Bitz, 2020). These examples emphasise the importance of a thorough discussion to prevent unintended censorship.

4.2 Reactions to the Black Lives Matter Movement

The second case example covers the *Black Lives Matter* (BLM) movement that gained public attention around May 2020, following the death of George Floyd. The case was heavily discussed on social media, fuelled by measures induced on society following the spread of coronavirus and the resulting increased use of the Internet for communication. The movement also triggered a discussion on discriminatory posts, hate speech, and verbal violence against minorities or suppressed groups on social media platforms (SZ.de, 2020). Social media platforms first emphasised the aspect of free speech, but later experienced pressure from the public, their customers (i.e., organisations that pay for advertisements), and their own employees. Reddit banned accounts spreading hate speech, an action that has been labelled as "deplatforming", followed by Twitter, Youtube, and Tiktok (Hurtz, 2020). Facebook, which had previously taken a less restrictive approach, declared that it would change its guidelines, following protests of its employees and threats from customers to withdraw their advertisements from the platform (Hurtz, 2020b). Twitter decided that it would delete posts or, in case they were against Twitter's guidelines but from an author of public interest, such as the US president, hide them behind a warning message. The delicacy of the action taken by the PSPs is underlined by some important considerations: The tension between the freedom of speech versus action taken against the spread of misinformation (often labelled as "censorship" by its contestants) has already been explained in the example of coronavirus. The questions raised under the pressure of the BLM movement underline similar problems: While presumably the general goal of banning hate speech and verbal violence is widely shared, the line between what is and is not allowed to be posted is difficult to define and risks being subject to opinion bias or temporary waves, which could result in unfair discrimination of non-mainstream opinions in their right to free speech. The sequence of events with respect to regulation of posts on the BLM movement illustrates this problem: instead of basing its activities on general rules that apply equally to all actors, Facebook only responded to criticism emerging from one opinion group, and gave way to pressure from employees and financial pressure from its advertisement customers. While it did resist governmental pressure, and so did Twitter when experiencing far greater pressure as a response to its ban of a post by the US president, a response to political pressures from opinion groups or financial pressures from advertisement customers does not yield an approach towards restricting verbal violence or hate speech that is applied equally to all users. Rather, it seems that Facebook only responded to public pressure. Claims have been made that the public pressure Facebook responded to yielded a restrictive situation, in which harmless posts were banned (SZ.de, 2020b). This practice might favour a specific opinion and gives way to claims of censorship and fuels conspiracy theories on information control.

4.3 The US Presidential Campaign

The third case, the US election campaign, has to be considered on the background of the BLM movement already described, since it also became a topic in the US elections. The already discussed warning message displayed on top of one of the US presidents' tweets resulted in a power battle between the US president and Twitter: The US president announced he would sign a decree in order to change the 1996 Communication Decency Act that disengages Internet platforms from any responsibility for the content generated by their users. It currently provides the basis for the business model of PSPs but, following the plans of the US president, should be changed to ensure freedom of speech and prevent any "censorship" by the PSPs "against conservative" opinions (Langer, 2020). However, the decree did not materialise. Nevertheless, the intervention of a political actor, the US president, in operational decisions of the platforms underlines their importance in the political process of Western countries and particularly the US. The case of the US elections is particularly interesting, since large PSPs are mostly subject to US jurisdiction. Therefore, the US is the one country in the world with the greatest influence on PSPs' practices, potentially being able to restrict or even shut down PSPs located in the US. As such, the US is a country that can influence PSPs' operation globally by means of national regulation, while other countries struggle to effectively regulate PSPs since they are beyond their direct jurisdiction. There are mechanisms employed by states, particularly by some European states or also the EU, that influence PSPs and that companies adhere to in order to avoid difficulties. Nevertheless, states have

limited scope in pressuring PSPs to comply with their regulations when acting on their own. The case of the US illustrates why PSPs might have to remain neutral from a state, in order to provide a political forum that is not subject to restrictions by a government; however, the emergence of hate speech and verbal violence also underlines that some sort of regulation is required nevertheless. PSPs have further underlined their will to remain neutral from state content providers by flagging accounts that are connected to states or politicians. For example, Twitter has started to flag accounts of state-influenced or state-owned media, such as specific Chinese or Russian content providers, in order to ensure transparency of content provision (NZZ.ch, 2020b and SZ.de 2020d).

4.4 Mitigation Mechanisms

The current subsection discusses some mitigation mechanisms on the background of the three cases illuminated in the previous subsections. First, Facebook explained that it will address problems of political advertisements early in 2020: Whoever would want to place such advertisements would need to undergo an additional registration and verification mechanism (Muth, 2020). These measures were aimed at increasing transparency by introducing an advertisement archive. They were inspired by experiences from previous elections and popular votes, such as the 2016 US presidential election, the Brexit popular vote in the UK, or the Irish referendum on abortion. The measures were aimed both at the US election and the EU elections in May 2020. One main focus was to prevent so-called *Dark Ads*, which are only displayed to very specific user groups and, therefore, bear the potential for misinformation while remaining hidden from broader public attention and scrutiny. The advertisement archive would make it possible for the public to trace political advertisements and access information such as the issuer's identity, the amount paid, and who an advertisement was targeted for. This new practice is in-line with PSPs acting as a global forum by increasing transparency and accountability, elements that are essential in the non-digital political discussion in liberal democracies. However, they raise important questions: is it sufficient that PSPs self-regulate? Who determines how far this regulation goes? Is there a need for democratically or otherwise legitimated control of measures are taken?

While the discussed transparency and accountability mechanism for political advertisements inherently implies Facebook sees itself as a political forum of high relevance, Facebook later announced a ban for political advertisements during the week preceding the election date in the US (Facebook, 2020). Facebook (2020) also defined clear (mis)information policies applied to statements on COVID-19 risks during the election, posts that might attempt to delegitimise the election's outcome, or premature claims of victory. These measures were probably inspired by concerns on the potential unrest such misinformation could cause in the political process. Similar steps would conventionally be considered within a state's legal code concerning the election process. However, in this case, the actions taken were imposed on a purely self-regulatory basis. Due to the turbulences around the election result in the US, Facebook announced to extend the ban on political advertisements and its other sanctions in order to avoid *confusion* during the process of the handover of power (Kamp, 2020 and Hatmaker, 2020b). The importance of these measures in terms of political stability and avoidance of the spread of misinformation and conspiracy theories has been emphasised by Kamp (2020). The action taken, however, did not stand under any particular national legislation. The cascade of events and actions outlined emphasises the claim of PSPs acting as a fifth estate (Dutton, 2020) by means of providing globally operating political and social forum. They also reveal the potential dependence on the good-will of PSP's when they are beyond a state's jurisdiction. The "power struggle" between PSPs and the US president on the handling of questionable posts made by the latter (SZ.de, 2020c) emphasise these aspects, while also underlining the need for PSPs to be somewhat independent from governmental influence.

A further attempt to resolve the regulation problem has been taken by the US lawmakers in November 2020: the heads of PSPs, such as Facebook and Twitter, had to answer questions during a hearing in the US Senate. Both Mr Zuckerberg (Facebook) and Mr Dorsey (Twitter) emphasised that a reform to legal mechanisms of content moderation might be required. They further stated that they implement different measures for content moderation (Isaac, and Browning, 2020). Twitter was more restrictive, banning accounts more quickly than Facebook. The tension between verifying information in order to avoid misinformation and providing a free and open forum under the principle of freedom of speech is handled differently; it is not supported by any national legislation. PSPs have come to the conclusion that some moderation is necessary on the background of the events outlined earlier (NZZ.ch, 2020).

While the self-regulatory steps outlined might be seen as a mitigation for the problems, their success is questionable. Reports have shown that previously banned accounts moved from the most popular PSPs to other, less restrictive PSPs: a platform called *Parler* specifically marketed itself as being less restrictive towards content and attracts mainly right-wing and conservative users and content providers (Their, 2020). Parler

claims to offer “real” freedom of speech while rejecting “techno-fascism” (Their 2020). However, this practice of Parler also gave room to misinformation and conspiracy theories, such as posts about an alleged “pandemic” being the explanation around the coronavirus pandemic. Parler’s community guidelines leave scope for interpretation and give precedence to the principle of freedom of speech in case review volunteers disagree. Such a loose enforcement of guidelines bears its problems. The importance of some kind of regulation is underlined by the case of verbal violence and misinformation against Kamala Harris: Facebook had to remove posts about US vice-president-elect Kamala Harris that were verbally violent. Facebook took the approach of deleting the posts, while not banning the groups that had allowed the spread of such posts (Clayton, 2020). The emphasis lies on moderating the content depending on specific criteria, while not generally banning users or groups from using a platform. As such, Facebook acknowledges the necessity and openness of its role as a global forum, but restricts some of the content in case it is too violent or breaches the limits of its hate speech definition.

Facebook has introduced a further mechanism to ensure the political independence of its content moderation decisions, which might be a first step towards implementing political platform neutrality: the *Facebook Oversight Board* provides users with an option for appeal of content moderation decisions (Levy, 2020). It has been called “Facebook’s Supreme Court” (Levy, 2020), providing para-state structures in terms of a judiciary for content moderation. Mark Zuckerberg has claimed “Facebook should not make so many important decisions about free expression and safety on our own” and Facebook further admits that “with our size comes a great deal of responsibility” (Clegg, 2020). The board’s members are funded by means of a separate *Oversight Board Trust*, which ensures the members’ financial independence from Facebook (Clegg, 2020). The board’s structure further prevents a national or cultural bias by involving members from more than 27 countries, speaking more than 29 languages (Clegg, 2020).

An example from the EU shows how transnational collaboration further enhances self-regulation: Meta Beisel and Kolb (2020) outline the reaction of the EU Commission’s Vice-President, Věra Jourová, upon identifying foreign powers, such as Russia and China, as being responsible for specific misinformation campaigns: the EU Commission now asks PSPs to provide a detailed monthly report, which outlines their self-regulatory activities. This ensures transparency and freedom of speech. Notably, even the Chinese-owned video platform TikTok participates in this voluntary process. The EU’s initiative provides an interesting example of transnational control, with an emphasis on transparent self-regulation, while providing little actual regulation; the EU takes an approach of non-regulation through transparency and potential of negative consequences in case the mitigation mechanisms are insufficient, i.e. it expects the PSPs to regulate themselves and provide detailed documentation about the mechanisms of self-regulation. Due to the EU’s structure, this oversight is democratically legitimized while omitting direct governmental or regulatory influence.

5. Conceptualisation of Political and Social Platform Neutrality

In this section, the concept of platform neutrality is formalised. PSPs provide global forums, due to the inherently global character of cyberspace (Stolz, 2020). Section 4 explained the relevance of PSPs for the functioning of political and societal discussion: PSPs have an impact on national politics while being global in nature. Various cases of problems and mitigation mechanisms have been discussed. This paper suggests that PSPs should be viewed as relevant actors in the global arena of international politics, as has been suggested by Kello (2017). Their role in influencing developments within states but also between states is plausible on the background of the cases discussed. PSPs offer a space where people can interconnect, generate and share

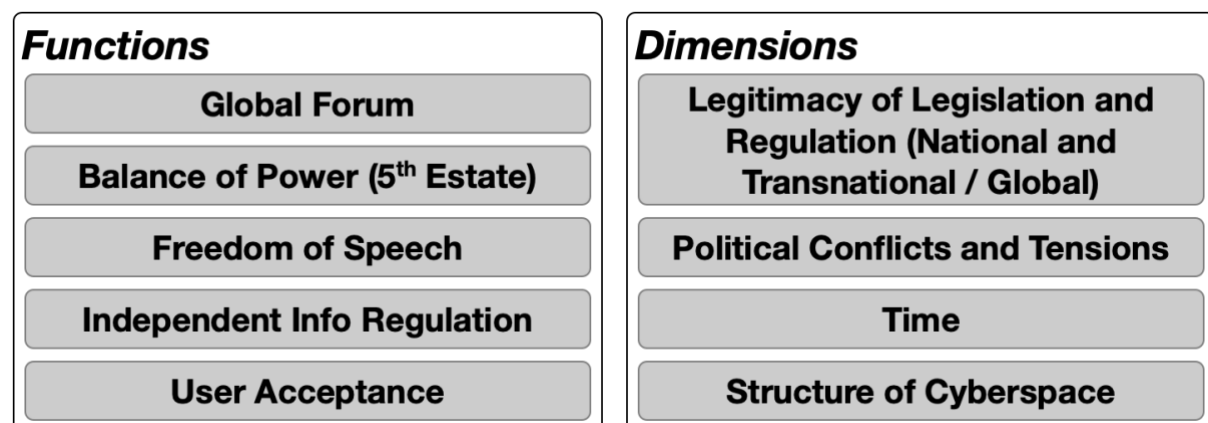


Figure 2: Functions and Dimensions of Platform Neutrality.

information, and instantly respond to content from other users in a public or semi-public manner.

The concept of *political* and *social* platform neutrality is inspired by state neutrality. PSPs, functioning as global actors, should be neutral from specific countries and political or social groups. This neutrality fulfils specific functions, which are related to problems discussed in Section 4 and are shown in Figure 2. *User Acceptance* considers the phenomenon of users switching to other platforms due to restrictions or restrictive practice. Neutrality of platforms should enable PSPs to remain trusted and, thus, accepted by their users while also maintaining a sufficient regime of information control, as contained in the function of *Independent Info Regulation*. This function includes effective measures against misinformation and verbal violence or hate speech that are unbiased and adhere to specific principles, which are applied equally and independently from any mainstream opinions or pressures from specific groups. Platform neutrality ensures that this regulation happens independently from governmental pressure or restrictive legal regimes present in some jurisdictions. Due to this independence from governmental or other pressures, platform neutrality further enables *Freedom of Speech*. A further function of platform neutrality is that of a *fifth estate* (Dutton, 2020), both within a country as well as in the global community; therefore, platform neutrality enables a balancing of powers both on a national and global level by means of providing a global forum. Neutrality further contributes to the success of these forums being adopted widely or even globally, which contributes a public good to the global community. Furthermore, the aspect of a global forum that is independent from a specific state jurisdiction increases credibility and trust in PSPs; e.g., foreign governments would not need to fear influence by the U.S. government when users access Facebook's services.

The dimensions relevant for Platform Neutrality are also listed in Figure 2. Platforms certainly depend on the structure of cyberspace; some countries, such as China, already contribute to a development that has been labelled as "splinternet", by means of restricting many global services. As such, platforms and their neutrality with respect to politics and countries will depend on the further developments of the global structure of cyberspace. Furthermore, the concept of Platform Neutrality will gradually develop over time, as has already been the case with the self-regulation of PSPs outlined in Section 4. Platform neutrality will need to prove itself as an effective instrument for the provision of a (global) forum in the times of increased political tensions; this development has so far been positive and into the direction of platform neutrality, which indicates that platform neutrality is indeed beneficial for the PSPs as well as for democratic societies. Finally, the question of legitimacy of any measures decided by PSPs is yet open; platform neutrality will depend on the trustworthiness of the measures taken by platforms in order to self-regulate. As such, there needs to be some source of legitimacy for the measures taken by platforms. The Facebook Oversight Board provides an example for establishing legitimacy of decisions: it is drawn from the expertise, independence, and diversity of its members. In general, legitimacy might be drawn from the effectivity of measures already experienced (e.g., experiences made with the Facebook Oversight Board's functioning), while some legitimacy might have to be further granted by means of establishing specific transnational or even international structures. The example of the EU's approach towards overseeing self-regulation of platforms is democratically legitimised due to the EU's democratic structure. A similar concept of oversight and potential minimal regulation of the independence of PSPs from states might also be implemented by international bodies, such as the UN. A collaborative and multilateral effort would presumably provide a high level of legitimacy not only for the self-regulatory measures of PSPs but also for the neutrality of PSPs; even in case a country disagrees with the practice of a PSP, it would be difficult to challenge its neutrality when the PSP is under global oversight and independent from a single country's direct influence.

6. Conclusion

This paper introduced the concept Platform Neutrality for PSPs due to their global operation and their international importance. While it relies on cases and developments in the real world and is inspired by the concept of state neutrality that has been effectively implemented over almost two centuries, further research required to establish the feasibility and effectivity of the concept. Some aspects of the concept are already being implemented currently by PSPs; other aspects, such as the idea of legitimacy through transnational or international bodies, require further investigation. Moreover, the concept needs to be discussed more broadly, including major PSPs and representatives of transnational and international organisations, in order to scrutinise current definitions and work towards a broad adoption of the model.

References

- AVAAZ (2020) 'Facebook's Algorithm: A Major Threat to Public Health', 19 August.
- Bitz, X. (2020) 'Twitter geht gegen Verschwörungstheoretiker vor', *SZ.de*, 22 July.

Clayton, J. (2020) 'Kamala Harris: Facebook removes racist posts about US vice-president-elect', *BBC News*, 16 November.

Clegg, N. (2020) *Welcoming the Oversight Board - About Facebook*, Facebook. Available at: <https://about.fb.com/news/2020/05/welcoming-the-oversight-board/> (Accessed: 21 December 2020).

Conseil National du Numérique (2014) *Platform Neutrality (57)*, 2014. Paris.

Denkler, T. (2020) 'Trump sagt Twitter den Kampf an', *SZ*, 28 May.

Dutton, W. H. (2020) 'The Fifth Estate: Canaries in the Institutions of Liberal Democracies', in Nagel, M. et al. (eds) *Politische Komplexität, Governance von Innovationen und Policy-Netzwerke. Festschrift für Volker Schneider*. Wiesbaden: Springer VS, pp. 59–65.

Facebook (2020) *New Steps to Protect the US Elections - About Facebook*, fb.com. Available at: <https://about.fb.com/news/2020/09/additional-steps-to-protect-the-us-elections/> (Accessed: 17 December 2020).

Facebook (2020) *New Steps to Protect the US Elections - About Facebook*, fb.com. Available at: <https://about.fb.com/news/2020/09/additional-steps-to-protect-the-us-elections/> (Accessed: 17 December 2020).

Gao, W. and Yang, Y. (2015) 'Chaining cyber-titans to neutrality: An updated common carrier approach to regulate Platform Service Providers', *Computer Law and Security Review*. Elsevier Ltd, 31(3), pp. 412–421.

Hatmaker, T. (2020) 'Facebook will put a new coronavirus info center on top of the News Feed | TechCrunch', *Techcrunch*, 18 March.

Hatmaker, T. (2020b) 'Facebook extends its temporary ban on political ads for another month | TechCrunch', *Techcrunch*, 11 November.

Hurtz, S. (2020) 'Facebook und Reddit: Keine Bühne für Rassisten', *SZ*, 17 July.

Hurtz, S. (2020b) 'Werbeboykott: Facebook steht unter Druck wie selten zuvor', *SZ*, 30 June.

Isaac, M. and Browning, K. (2020) 'Zuckerberg and Dorsey Face Harsh Questioning From Lawmakers - The New York Times', *The New York Times*, 18 November.

Jan Krämer and Schnurr, D. (2018) 'Is there a need for platform neutrality regulation in the EU?', *Telecommunications Policy*. Elsevier Ltd, 42(7), pp. 514–529. doi: 10.1016/j.telpol.2018.06.004.

Kamps, L. (2020) 'Facebook bereitet sich auf eine Zeit ohne Gewinner vor', *Netpolitik.org*, 8 October.

Kello, L. (2017) *The Virtual Weapon and International Order*, *The Virtual Weapon and International Order*. Yale University Press.

Kormann, J. (2020) 'Facebook löscht erstmals Trump-Video zum Coronavirus', *NZZ*, 6 August.

Langer, M.-A. (2020) 'Trump rächt sich mit einem Dekret an Twitter und anderen sozialen Netzwerken', *NZZ*, 29 May.

Levy, S. (2020) 'The Plain View: Facebook's Oversight Board', *WIRED*, 10 February. Available at: <https://link.wired.com/view/5d727748a777390d4a148d90cwggx.4cfh/deedc305> (Accessed: 21 December 2020).

Meta Beisel, K. and Kolb, M. (2020) 'EU will härter gegen Desinformationen vorgehen', *SZ*, 10 June.

Muth, M. (2020) 'Wie Facebook unlautere Wahlwerbung verhindern will', *SZ*, 29 March.

NZZ.ch (2020) 'Soziale Netzwerke und US-Wahlen: Die Chefs von Facebook und Twitter stellen sich den Fragen der Senatoren', *NZZ*, 18 November. Available at: <https://www.nzz.ch/technologie/us-wahlen-das-sind-die-herausforderungen-fuer-facebook-und-co-ld.1557220> (Accessed: 17 December 2020).

NZZ.ch (2020b) 'Twitter versieht staatsnahe Nutzerkonten mit Symbolen', *NZZ*, 7 August. Available at: <https://www.nzz.ch/panorama/twitter-versieht-staatsnahe-nutzerkonten-mit-symbolen-ld.1570160> (Accessed: 21 December 2020).

Spring, A. (2014) *The international law concept of neutrality in the 21st century. An analysis of contemporary neutrality with a focus on Switzerland*. Edited by T. Cottier et al. Zürich / St. Gallen: Dike.

Stauffacher, R. (2020) 'Studie von Avaaz zu Covid-19: Facebook versinkt in den Fake-News', *NZZ*.

Stauffacher, R. (2020b) 'Wie sich Facebook und Co. in der Corona-Krise als Helfer in der Not profilieren', *NZZ*.

Stolz, M. (2019) 'On Neutrality and Cyber Defence', in Cruz, T. and Simoes, P. (eds) *18th European Conference on Cyber Warfare and Security*. Coimbra: ACPI, UK, pp. 484–491.

Stolz, M. (2020) 'Cyberintelligence and Cyberdefence: Opponents or Accomplices', in *16th International Conference on Cyber Warfare and Security*. Tennessee: ACPI, USA.

SZ.de (2020) 'Zuckerberg will Umgang mit umstrittenen Posts prüfen', *SZ*, 6 June. Available at: <https://www.sueddeutsche.de/digital/facebook-rassismus-trump-1.4929164> (Accessed: 15 December 2020).

SZ.de (2020b) 'Facebook geht gegen "Blackface" und Antisemitismus vor - Politik - SZ.de', *SZ*, 12 August. Available at: <https://www.sueddeutsche.de/politik/facebook-blackface-zwarte-piet-1.4997003> (Accessed: 15 December 2020).

SZ.de (2020c) 'Facebook und Twitter gehen gegen Trump-Postings vor', *SZ*, 19 June. Available at: <https://www.sueddeutsche.de/digital/trump-facebook-twitter-1.4941126> (Accessed: 17 December 2020).

SZ.de (2020d) 'Twitter kennzeichnet ab sofort staatsnahe Medien', *SZ*, 7 August. Available at: <https://www.sueddeutsche.de/digital/twitter-staatsmedien-warnhinweis-1.4992236> (Accessed: 21 December 2020).

Thier, J. (2020) 'Coronavirus bringt Facebook in die Bredouille', *NZZ*, 31 March.

Thier, J. (2020b) 'Weil Twitter und Facebook nicht alles erlauben, kommt jetzt ein neuer Spieler auf den Markt', *NZZ*, 8 August.

Vincent, J. (2020) 'YouTube is adding information about COVID-19 vaccines to its fact-check panels - The Verge', *The Verge*, 18 November. Available at: <https://www.theverge.com/2020/11/18/21573019/youtube-information-panels-fact-check-boxes-covid-19-vaccination-misinformation> (Accessed: 14 December 2020).

Appendix D

Published Paper: *Platform Neutrality and the Global Balance of Powers*

The following paper [165] was published at the 2021 *International Conference on Computational Science and Computational Intelligence* in the *Symposium on Social Network Analysis, Social Media, & Mining* track (CSCI-ISNA 2021). It has been presented at conference in December 2021 and published in 2022.

Platform Neutrality and the Global Balance of Powers

Marcel S. Stolz

Department of Computer Science

(Cybersecurity Analytics)

University of Oxford

Oxford, United Kingdom

marcel.stolz@oriel.ox.ac.uk

Abstract—This paper defines *platform neutrality* as a concept for large technology companies, most notably, social media platform providers. It is deduced from the concept of state neutrality, and acknowledges societal and political functions as well as state-like structures these companies have put into place. The paper argues that recent developments demonstrate a convergence of social media towards platform neutrality. It explains the benefit of platform neutrality both for businesses as well as societies.

Index Terms—social media, facebook, twitter, youtube, neutrality, balance of powers

I. INTRODUCTION

Large technology companies have become significant global actors and have been found to revolutionise the conventional *Westphalian system of states* [7], which defined states as the single entity of sovereignty in an anarchic system of states. International Relations Theory traditionally considers states to be in a “constant state of competition” [10] and it is not clear what role large technology companies take in the cyber era. Some scholars have suggested that globally operating technology companies should be considered as entities similarly relevant to states for international relations and global cooperation. [7]. On the background of recent developments, particularly during the coronavirus pandemic and on social media platforms, this paper analyses the role of large technology companies and addresses some of the imminent problems encountered during the last months and years, such as the tension between freedom of information and censorship, the balance between regulation and self-responsibility, or the relation between social media providers and the state.

This paper focuses on examples from social media platform providers, as they yield the most prominent cases for analysis. In order to explore their role, this paper follows an approach of analysis, empirical examples (“*case studies*”) and reflection. It builds on and further develops the concept of *platform neutrality* [18], in order to conceptualise how the role between technology providers and the global community may be rationalised. It is deductive and exploratory. The concept is partially informed by past research based on case studies [18] and on research analysing the potential of *state neutrality* in the cyber era [16].

The remainder of this paper is structured as follows: Section II outlines the specific context of the discussion. It explains the concepts in International Relations Theory and Social Science, and how the emergence of cyberspace has influenced these concepts. Thereafter, Section III outlines the conventional principles of neutrality and explains how these have developed from conventional state neutrality towards state neutrality in the cyber era, and how the neutrality concept may be applied to global non-state actors by defining *platform neutrality*. This is done by deductive reasoning. A subsequent case study in Section IV explains how social media platforms indeed do converge towards a state of platform neutrality. Finally, Section V draws conclusions and outlines possible future work.

II. CONTEXT OF NEUTRALITY AND GLOBAL STABILITY

Since this paper addresses the role large technology companies may take in a global context and in relation to states, it is useful to consider the disciplinary context of the discussion. International Relations Theory conceptualises the inter-state relations and global power dynamics. The most common model for reasoning is referred to as the *Westphalian system of states*, as for example outlined by Nye [10]. It considers states to be the sole sovereign entities in an anarchic systems of states¹ and considers them to be in a state of constant competition. Kello claims that this system has been revolutionised by the emergence of cyberspace as a novel dimension of security, and that large technology companies have become actors with similar relevance as states in the global arena. The reflections in this paper rely on this approach.

Furthermore, a common concept of discussion in international relations is the idea of a Balance of Power between sovereign units of the global arena. As Nye outlines [10], a balance of power may support global stability in an anarchic system of states, since it distributes power between different actors and may ensure that one single actor cannot become (too) dominant over the others, or act as a hegemon. Furthermore, *Balance of Power Theory* outlines the idea that states will take actions to avoid any one state from becoming too powerful, in

¹In particular, this is the common conception in the *realist* perspective of International Relations Theory, see Nye [10].

order to balance power. The concept of neutrality emerged from balance of power considerations in the 19th century following the napoleonic wars and was defined at the *Concert of Europe* [10, 13, 16, 19]: the five major European powers (Russia, Prussia, Britain, Austria, and France) defined that the geostrategically important territory of Switzerland in the Alps should not be controlled by any of them. Instead, it should remain neutral.

As the focus of this paper lies on global technology companies, particularly social media platform providers, a further important concept of International Relations Theory is that of *transnational actors* and *complex interdependence* [10]. Large technology companies may be considered as transnational actors, as outlined by Nye, and in a world of complex interdependence, their global role and their relation to states is of interest, as they also influence the internal functioning of states. Dutton has outlined how social media platforms—or rather, their users—are a *fifth estate* [5] within (democratic) countries:

“The collectivity of individuals who use the Internet to hold institutions more accountable – the Fifth Estate - [...] opens new ways of making government, media and other institutions more socially accountable.”

The influence of social media platforms on societies, politics, and security has been demonstrated by numerous examples [18]. During the Coronavirus pandemic, social media has taken on an even more prominent role in interconnecting people.

The emergence of technology companies as transnational actors, therefore, yields an interesting example which combines the role of an actor relevant for national politics with the role of a globally relevant actor for international relations. The upcoming sections explain how the concept of neutrality has changed with the emergence of cyberspace and how it may be applied to large technology companies, and how, on this background, platform neutrality is being implemented by large technology companies, with particular relevance for social media companies.

III. FROM STATE NEUTRALITY TO PLATFORM NEUTRALITY

As outlined in the previous section, state neutrality is a concept introduced and explained on the background of balance and distribution of power theories. It contributes to global stability by means of declaring a strategically important asset—conventionally the territory and infrastructure of a state—as independent from large powers’ direct control.

A. State Neutrality

State neutrality has been conceptualised by the definition of specific functions it yields for the implementing state as well as the global community, most notably by means of the example of Switzerland. Switzerland is the longest lasting example of state neutrality, as it has been continuously implemented and evolved since 1815. A history of neutrality

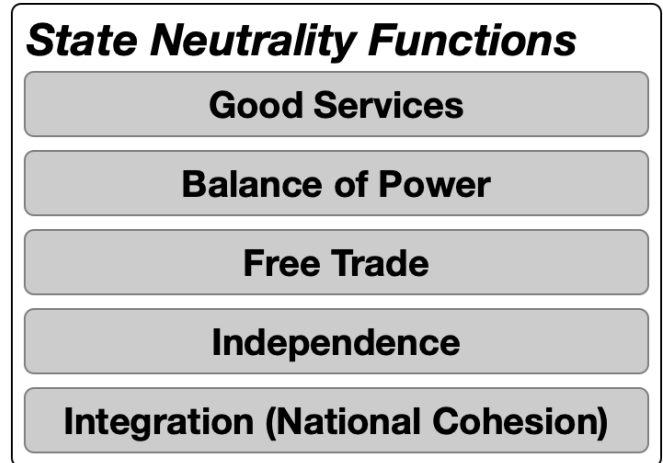


Fig. 1. Functions of State Neutrality [16, 19]

has been, for example, outlined by Suter [19] and its functions defined by Riklin [13]. A graphic outlining the functions is shown in Figure 1 (from Stolz [16]) and the functions shortly summarised in the following.

Integration denotes neutrality as a useful tool for (ethnically or culturally) diverse communities, e.g., in order to prevent a split in society, which could be caused by political tensions between neighbouring countries connected with the respective groups of a country. *Independence* denotes political independence from major political blocks and alliances in the international context. It reduces the risk to be drawn into a conflict connected to another member of an alliance system. *Free Trade* identifies a similar aspect, with a stronger focus on economy: In a world divided into economic blocks, it ensures that trade is possible with any and all of these blocks. *Balance of Power* denotes the geostrategic connotation of Swiss neutrality already outlined, where a neutral actor may contribute to a balance of power. *Good Services* are related. On the one hand, they include the provision of diplomatic or supervisory services for third parties (e.g., the US interests section located at the Swiss embassy in Teheran, or the Neutral Nations Supervisory Commission at the intra-Korean armistice line). On the other hand it includes hosting of international organisations, such as the United Nations or International Committee of the Red Cross (ICRC), or the supervision of international treaties, such as the Geneva Conventions.

Stolz elaborates, how the concept of state neutrality may evolve in the cyber era: Neutral countries could provide good services, such as hosting a forensic laboratory for the analysis of the origin of cyberattacks, similar to the case for biological and chemical weapons. Furthermore, neutral actors may be important when facilitating cyber norms on use of cyberspace for conflict or propaganda. He further elaborates on the difficulty of responding to cyber incidents originating from state actors [17] and how current practice works de-escalative, counter-intuitively to Buchanan’s *Cybersecurity Dilemma* [4].

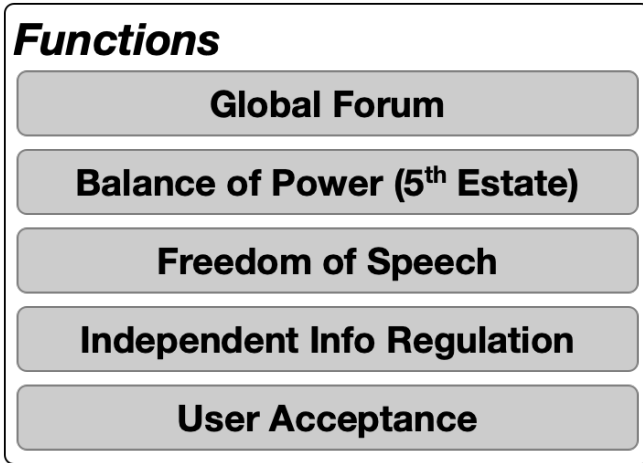


Fig. 2. Initial definition of *platform neutrality* [16]

B. Platform Neutrality

The concept of state neutrality evolves into the first inductive definition of *platform neutrality* [18]: the functions are transferred to social media platform providers, as shown in Figure 2. This definition relies on empirical evidence from three case studies for its justification:

- 1) The discussion around misinformation and censorship on social media, and appropriate countermeasures, following the first “lockdown” of the Coronavirus pandemic in 2020;
- 2) the discussion on hate speech and censorship on social media, and appropriate countermeasures, following the emergence of the *Black Lives Matter* protests in the United States and further countries in 2020;
- 3) The United States presidential election campaign in 2020 and the subsequent United States Capitol attack in January 2021, with a focus on political ads control and balance of power between technology companies and their host state.

The different functions of platform neutrality are derived from the respective functions of state neutrality: *User Acceptance* describes the requirement of neutrality for a broad user base. Users who feel that the platform they use supports a certain political view or narrative will not trust this platform and boycott its use by switching to a different social media provider. However, the value of social media platform is derived from their universality: only when they provide a space considered equally open to any political groups and individuals, the platforms may function as a *global forum*. Furthermore, the platforms themselves have an interest in appealing to the broadest possible user range due to economic incentives. Similarly, users will be inclined to use a platform that most of their friends use, since they aim to connect with all of their friends through the same platform. In this sense, user acceptance might be considered a similar principle to state neutrality’s integration function. *Independent Info Regulation* denotes the possibility to detach information

regulation from the control of a government or state. In order to avoid censorship or the control of media and information—as considered necessary for liberal democracies—the information should not be controlled directly by a state. Conventionally, the oversight over information control mechanism would lie with a judiciary system, following a state’s legislation. However, on a global platform, such as social media, such a mechanism has limited impact: While social media platform providers may be forced by national legislation to abide by local (information) legislation, in practice, users may easily circumvent such legislation if policies are only based on geo-blocking and not applied universally by a social media platform provider. It is therefore more reasonable, if platform providers define and implement rules and principles for the contents that may be shared on their platforms globally and in a self-regulated manner, relying on a broad consensus of countries. This also prevents that a single state may control online information and ensures freedom of information, while maintaining a basic set of principles, for example to avoid hate speech or misinformation. This function is, therefore, closely related to *Freedom of Speech* and the related considerations have already been outlined. The *Balance of Power* function relates both to its counterpart in state neutrality in terms of balancing power on a global level as well as within a state: On the one hand, neutral platforms may act in a balancing power between states, since they provide a forum and define the rules for contents that users (including state entities or members of government) may post. On the other hand, this also provides a balance within a state, between entities such as the populus and a government, which would traditionally have been regulated by means of national legislation. *Global Forum*, finally, is closely related to the balance of powers: neutrality enables platforms to provide a global forums for all on an inter- and intra-state level.

IV. SOCIAL MEDIA CONVERGENCE TOWARDS PLATFORM NEUTRALITY

Having outlined the concept of state neutrality in cyberspace as well as the derived concept of platform neutrality, this section outlines how the concept of platform neutrality should further be evolved and reflects on a convergence of developments towards platform neutrality, reflecting on recent developments on social media platforms.

A. Amended Definition of Platform Neutrality

Figure 3 outlines an updated version of the functions of platform neutrality, based on the original definition shown in Figure 2: *Universality* has been found to be a more fitting term, since it denotes that neutrality enables platforms to be perceived as universal, i.e., suitable for all user groups. A platform governed or influenced predominantly by one state could be perceived to be politically biased towards a specific user base. A platform that credibly upholds neutrality in the sense of independence, should yield an environment considered universal, i.e., suitable for all users, regardless of their political or any other background. *Self-regulation*

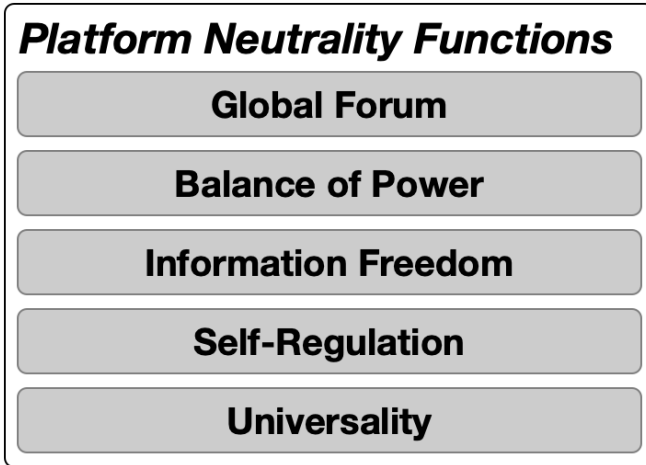


Fig. 3. Amended definition of Platform Neutrality

relates to the aspect that platforms should not necessarily rely on regulation by one single state or adopt its content rules depending on where users access the platform from. As has been outlined previously, geo-blocking is of limited use on the Internet: contents that are limited, altered, or blocked in one geographic location may easily be accessed by making use of tools, such as Virtual Private Networks (VPNs) [1, 2, 20], Secure Shell (SSH) tunnels [24], or TOR browsers [24]. Nevertheless, social media platform have an interest in defining and enforcing basic rules for user content and user behaviour, as has been outlined by Stolz [18], in order to avoid scandals and a negative reputation and in order to ensure universality of their platform, i.e., in order to appeal to a widest possible user base. While platform service providers might not be subject to a single state's legislation in most cases, they do nevertheless give way to pressure from some individual states and groups of states, such as in supranational organisations (e.g., the European Union). Therefore, while platforms do and should regulate themselves in terms of the concept of platform neutrality, they do this in the manner of a dialogue with societies, movements, and states, in order to achieve universality. *Information Freedom* denotes the function of neutral platforms enabling a space that might be more free than a nationally regulated information space. On the one hand, this may be useful for citizens and movements in countries where information is subject to state control. On the other hand, this does not mean that any information may be shared; misinformation, for example, may be limited by a platform, as may attempts of promotion of violence or hate speech. However, since this is done in a self-regulatory manner, platform neutrality ensures a wider level of information freedom and a level of control of what may or may not be said that may be deemed more independent from state-controlled information legislation. As such, neutral platforms may be considered important facilitators for critical debates within and across societies and countries. The notion of *Balance of Power* does not differ from its original definition.

It includes the idea of a facilitator of a *fifth estate* within a country as well as a balancing factor between states in the information space of cyberspace.

B. Deductive Reflection and Verification of the Concept of Platform Neutrality

Subsection III-B outlined the initial definition of the term *platform neutrality*. The research references followed an inductive approach for this purpose, as outlined by Lamont and Boduszynski [8]; i.e., the theoretical concept of platform neutrality has been generated from empirical observation. The current section aims at following a deductive approach; i.e., the theoretical (amended) proposition for the concept of platform neutrality is tested to see whether it holds true with respect to further empirical observation. The empirical observation should not substantially overlap with the previous observations used for the inductive approach, in order to avoid a logical loop. Therefore, empirical examples that have already been used in the initial platform neutrality paper are specifically marked.

C. Empirical Examples

This subsection outlines a number of empirical examples relevant to the theoretical concept of platform neutrality. While the list is not exhaustive, the examples have been selected according to their relevance for platform neutrality and aim to illustrate a continuity of developments on the basis of the tension between traditional state control and the emergence of large technology companies as a relevant global actor. The empirical examples are listed in the following. Examples that have already been referred to are highlighted and referenced to the initial paper defining platform neutrality.

- 1) 2011 Arab spring: promotion of peaceful and violent uprisings against governments in Arab countries through social media; [18]
- 2) 2020 debate on misinformation and censorship with respect to the coronavirus pandemic; [18]
- 3) 2020 debate on hate speech, encouragement of violence, and censorship on the background of the Black Lives Matter (BLM) movement; [18]
- 4) 2020 discussion and measures with respect to the US presidential election campaign and social media ad campaigns; [18]
- 5) implementation of a review body for content moderation on Facebook; [18]
- 6) 2021 United States Capitol attack and blocking of Donald Trump's accounts;
- 7) 2021 blocking of *Russia Today's* Youtube channel;
- 8) usage of Twitter by the Taliban during the 2021 fall of Kabul (Afghanistan).
- 9) effect of Twitter on international diplomacy, exemplified by deescalation of diplomatic tensions in Turkey after tweet by US Embassy.

The first five examples listed have already been thoroughly discussed and outlined by Stolz [18] and have informed the initial definition of platform neutrality. While social media

companies have taken different approaches to addressing the tension between freedom of expression and necessity for self-regulation in order to avoid unwanted consequences (e.g., violence or hate speech), they follow a tendency towards a principle that attempts to reduce the amount of blocked content as far as possible; many social media companies only block or delete content in very clear cases of abuse. In cases where content is questionable but does not have a clearly abusive connotation, the approach seems to follow a principled of “mature social media citizenship”: users are informed that information displayed or expressed by other users might be contentious and provided with resources, which they may consult in order to access factual background information about a topic. This tendency expresses the benefit of platform neutrality with respect to information and political discussions: the self-regulation tends to be aimed at the necessary minimum, while attempting to avoid unnecessary censorship. By this practice, information freedom is upheld as far as reasonably possible. The social media companies take on a clear role of balancing power between governmental information control and users’ interests in free and open discussion and access to information. This enables the platforms to function as global forums, either for national or transnational information exchange and debate; universality is embraced as a principle in that the platform providers do not specifically aim at discriminating against any particular political group as long as no proof of deliberate spread of false information or abusive, hateful, polemic, or violent language is identified.

List item 6 is a further example of how social media providers’ practice converges towards platform neutrality: After the 2021 US Capitol attacks, social media companies came to be at the centre of public attention [15]. It was claimed to have a direct connection with developments on social media and, more specifically, the engagement of former US President Donald Trump on social media. It is a particularly important example, demonstrating how activities on social media imminently led to real-world violence. Furthermore, it may be juxtaposed to list item 1 in order to underline the importance of platform neutrality: While the developments during the Arab spring were predominantly seen as positive in the Western world, since they were perceived as pro-democratic and supportive of Western ideals, they are comparable to the developments in January 2021. Also during the Arab spring, groups connected through social media emerging not only in peaceful protests but also violent action. On the other hand, the US Capitol attacks of January 2021 were seen as critical by the majority of Western media. Platform neutrality suggests that developments on social media should be treated equally with respect to their potential for violence, regardless of the political aims of or sympathy with a particular group. In this sense, platform neutrality is also closely comparable to the conventional state neutrality. Furthermore, the subsequent handling by social media illustrates the effectiveness and usefulness of *Self-Regulation* by social media providers: Social media accounts deemed responsible for the escalations were subsequently blocked or banned completely, including

the account of former US president Donald Trump [14]. While Twitter made its decision permanent without further possibility for review, Facebook redirected its decision to its independent Oversight Board for review. The decision was confirmed, although the Oversight Board decided that a mandatory review period for the decision had to be put into place, such that the decision could be further reviewed after two years [9, 12]. While Twitter has not implemented a body similar to Facebook’s Oversight Board, it launched and enhanced its *Birdwatch* service, a community-based approach for managing misinformation [3]. Both the Oversight Board and Birdwatch are examples of how technology companies approach Self-Regulation, in order to maintain their credibility and provide a foundation for unbiased decisions with respect to information control, while acting independently from direct state involvement. The examples underline the role of technology companies with respect to the function of Balance of Power.

List item 7 further illustrates that information control by social media also bears relevance outside the United States and English speaking countries: Russia Today’s (RT) German Youtube channel had been banned following repeated spreading of disinformation about the coronavirus pandemic [23]. The example amplifies the importance of independence of social media companies, as the banning was followed by tensions between Russia, Youtube and threats of banning German journalists from Russia in return. The example may illustrate how Youtube balances the power between states and their influence on societies abroad, while applying self-regulatory rules and principles to its users.

List item 8 illustrates how Twitter functioned as an important facilitator of information following the fall of Kabul and collapse of the Afghan government in August 2021. A Twitter channel named *Civilian Casualty Prevention and Complaints Commission of the Islamic Emirate of Afghanistan*, which had been set up earlier in the year, served the Taliban both in taking control in a state of chaos but also reducing chaos in an environment of power vacuum [6]. It underlines how social media platforms are not only an essential actor on the inter- and intra-state level but also when a state no longer exists. The functions of Global Forum and Balance of Power (between old and new government) as well as Universality (since Twitter was used by US / allied users as well as the Taliban) are the ones most imminent from this example.

List item 9 further illustrates how a tweet from the US Embassy in Turkey allegedly reduced diplomatic tensions between the Turkish government and the West [21]: Preceding the tweet, eight high-ranking Western diplomats had been accused of interference in internal affairs and threatened with expulsion by the Turkish government. Despite the ambiguity of the tweet, it was considered that it was a sign of “backing down” by the Turkish side. This example shows how social media functions as a Global Forum, not only for individuals but also for state affairs between nations. Would social media platforms experience stronger state control, their role as provider for such a forum would need to be questioned, as well as their

universality with respect to participation of a wide range of state-level actors in the respective social media platform.

D. Convergence towards Platform Neutrality

From the examples listed and analysed in the previous section, we derive a convergence towards the principle of platform neutrality. Furthermore, the examples illustrate the applicability of the theoretical concept as a tool for analysis and interpretation for the role of social media for societies and the international communities.

A further indicator for convergence towards a state of platform neutrality is the European Union's planned *Digital Services Act* (DSA) [23]: While it aims at improving collaboration between a state-backed body (the European Union) and social media platform providers, it also acknowledges the difficulty of regulating the contents of these platforms nationally. Contents should not be blocked in one single country, but regulated in collaboration with platform providers through a harmonised framework. Hence, an approach is followed that respects the specific characteristics of cyberspace where the actions of one single state have little weight. Furthermore, Věra Jourová, Vice President of the European Commission for Values and Transparency, has emphasised the importance of collaboration with service providers [11, 22]: The DSA, therefore, emphasises transparency and requires platform providers to report their principles and rules for approaching problems, such as misinformation, hate speech, encouragement of violence, etc. According to Jourová, such an approach should encourage technology companies to respond in a self-regulatory manner to emerging problems; while the state (or the EU) could attempt to regulate, such an approach avoids a splintering of social media platform contents, which would disrespect the specific characteristics of cyberspace.

V. CONCLUSIONS AND FUTURE WORK

This paper has outlined how the concept of platform neutrality has evolved from conventional state neutrality. It further enhanced the theoretical definition of the concept of platform neutrality and analysed its applicability to current developments. While clear indicators exist that the evolution of Western social media companies converges towards platform neutrality, a more thorough analysis would be required that juxtaposes the concept to the development of "nationalised" social media platforms, such as those available in China. Furthermore, this paper focused on social media platforms as the most prominent example of globally acting technology companies, whose relation to the state deserves attention. However, platform neutrality has been defined as a concept applicable to large technology companies more generally; it remains to be analysed how this concept may be applied to such companies in a broader sense and such an analysis should be backed by further empirical evidence.

We conclude that the concept of platform neutrality is a useful tool for a better understanding of the power dynamics between users, societies, states, and social media platforms. Further work is required with respect to the general applicability of the

concept for large technology companies and a should consider how the concept incorporates nationalised (i.e., non-neutral) platforms, such as those common in China.

REFERENCES

- [1] 4 Ways To Access Sites in China If You're Already There in 2021, 9 2021.
- [2] Why VPNs Are Illegal in China and How to Get Around It, 10 2021.
- [3] Anthony Ha. Twitter's Birdwatch fights misinformation with community notes — TechCrunch, 1 2021.
- [4] Ben Buchanan. *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press, 2017.
- [5] William H Dutton. The Fifth Estate: Canaries in the Institutions of Liberal Democracies. In Melanie Nagel, Patrick Kenis, Philip Leifeld, and Hans-Jörg Schmedes, editors, *Politische Komplexität, Governance von Innovationen und Policy-Netzwerke. Festschrift für Volker Schneider*, chapter 7, pages 59–65. Springer VS, Wiesbaden, 2020.
- [6] Erin Gallagher. Tweet: The current pinned tweet of the "Civilian Casualty Prevention and Complaints Commission of the Islamic Emirate of Afghanistan" contains WhatsApp numbers to contact various provincial directors. US social media platforms are being used as a Taliban , 2021.
- [7] Lucas Kello. *The Virtual Weapon and International Order*. Yale University Press, New Haven, 2017.
- [8] Christopher K. Lamont and Mieczyslaw M. Boduszynski. *Research Methods in Politics and International Relations*. SAGE PUBLICATIONS, Los Angeles, 2020.
- [9] Marie-Astrid Langer. Niederlage für Donald Trump: Facebook muss den früheren Präsidenten vorerst nicht wieder auf seine Plattform lassen — NZZ, 5 2021.
- [10] Joseph S Nye and David A Welch. *Understanding global conflict and cooperation : an introduction to theory and history*. Pearson, Boston, tenth edition, 2017.
- [11] NZZ.ch. EU-Kommissarin warnt Facebook-Führung vor negativen Auswirkungen — NZZ, 3 2018.
- [12] Philipp Gollmer. Trump-Sperre auf Facebook: Account bleibt vorerst gesperrt, 6 2021.
- [13] Alois Riklin. *Funktionen der schweizerischen Neutralität*. Institut für Politikwissenschaft, St. Gallen, 1991.
- [14] Salvador Rodriguez. Trump Twitter account locked following video addressing Capitol rioters, 1 2021.
- [15] Sheera Frenkel. How The Storming of Capitol Hill Was Organized on Social Media - The New York Times, 1 2021.
- [16] Marcel Stolz. On Neutrality and Cyber Defence. In Tiago Cruz and Paulo Simoes, editors, *18th European Conference on Cyber Warfare and Security*, pages 484–491, Coimbra, 2019. ACPI, UK.
- [17] Marcel Stolz. Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries 3 . Conceptualisation of Operations in Cyberspace. In *16th*

International Conference on Cyber Warfare and Security, pages 345–353, Online, 2021. ACI, UK.

- [18] Marcel Stolz. Platform Neutrality – A Solution for the Social Media War? In *16th International Conference on Cyber Warfare and Security*, pages 336–344, Online, 2021. ACI, UK.
- [19] Andreas Suter. Neutralität. Prinzip, Praxis und Geschichtsbewußtsein. In *Eine kleine Geschichte der Schweiz*, pages 133–188. Suhrkamp, Frankfurt (Main), 1998.
- [20] SwitchVPN Team. Is It Legal To Use A VPN In China In 2021?, 6 2021.
- [21] sz/afp. Tweet entschärft Botschafter-Streit – Erdogan sieht sich als Sieger — Der Bund, 10 2021.
- [22] SZ.de. EU-Justizkommissarin Věra Jourová - "Ich habe ein großes Problem mit Anonymität" - Wirtschaft - SZ.de, 4 2018.
- [23] sz.de. Reaktion auf die Youtube-Sperre von RT DE - Medien - SZ.de, 9 2021.
- [24] TOR Project. How to circumvent the Great Firewall and connect to Tor from China? — Tor Project — Support.

Appendix E

Interview Forms and Ethics

This Appendix provides an overview of information relevant for the CUREC¹ ethics approval process for interviews used in this thesis and the structure used for the conversation with interviewees. Since also interviews from the mini project of the first year of the CDT² were used, the respective ethics approval number is listed below. It was updated twice for this thesis. A further, fresh ethics approval was requested and granted later during the research process. The respective CUREC approval reference numbers are:

1. **R50465/RE001;**
2. **R50465/RE002;**
3. **R50465/RE003;**
4. **CS_C1A_021_042.**

The interviews conducted are semi-structured. Where the sole focus of the interviews lay on state neutrality the approach outlined in Section E.1 was used. For interviews addressing both platform and state neutrality the structure listed in Section E.2 was used as a foundation.

E.1 Interview Structure for State Neutrality

¹Central University Research Ethics Committee, see: <https://researchsupport.admin.ox.ac.uk/governance/ethics/committees/curec>

²Centre for Doctoral Training in Cybersecurity.

Sample of interview questions for State Neutrality in Cyberspace.

The interview will be semi-structured. As such, it will follow a structure similar to the following but is open to any comments or topics that may arise in the flow of the conversation.

1. Reminder of consent form etc.
2. Remind interviewee of my background and what research I am conducting.
3. What background does the interviewee have in terms of IT (policy)? What is his background on legislation making / international politics?
4. What is Switzerland's traditional role as a neutral country, from the view of the interviewees?
5. Why, in the opinion of the interviewee, is this neutrality important for Switzerland?
6. Why is Switzerland important as a neutral country in the global community? What role does it play?
7. What capabilities does Switzerland currently have in the cyber landscape? What capabilities should it have?
8. What cyber capabilities are important to Swiss citizens and to Swiss business?
9. In what sense is the aspect of neutrality important in cyber space? Is this a matter of internal politics or does it also influence the global role of Switzerland?
10. What should be the aim of the Swiss government and the Swiss industry for a positioning in the global cyber community?

E.2 Interview Structure for Platform and State Neutrality

Platform and state neutrality interviews

Marcel Stolz, DPhil: Neutrality in Cyberspace

Aim: Many of the considerations in my DPhil are analytical and theoretical. I also provide empirical case studies in order to outline the problem scope of platform or state neutrality in cyberspace. In order to underline some of my considerations and add valuable aspects, I would like to contribute around 10-15 qualitative semi-structured interviews.

As the methodological basis I use:

Svend Brinkmann: *Unstructured and Semi-Structured Interviewing*, in: The Oxford Handbook of Qualitative Research. Edited by Peter E. Nathan.

Christopher Lamont & Mięczyław P. Boduszuński: *Research Methods in Politics and International Relations*. SAGE Publications Ltd.

Some interviews, mainly on state neutrality in cyberspace, have already been conducted earlier; so the focus in this document is stronger on platform neutrality.

Experts are typically from a business or organization affected by the considerations of platform or state neutrality in cyberspace or a relevant background, such as: ICRC, UN, EU, Facebook, Twitter, Google / Youtube, TikTok, Parler, Reddit, Professors as independent experts in the field, etc.

Structure of the conversation

- Background of the person in their own words; their role within their organisations / as an expert. About their organization and its values, what is important to them.
- What are the benefit of online platforms? What problems do we currently face?
- How effective are current approaches, and what shortcomings do they have?
- Explanation of the concept of neutrality in their own words -> What could it mean? What connotation does the word “neutrality” bring to their minds with regards to social media / tech platforms and the problems of advantages identified?
- Explanation by interviewer of what our concept of neutrality consists of
- Potential / benefit of platform neutrality for:
 - Business
 - Users
 - States
 - The global community
 - Third parties
- Evaluate what parts of the concept might be useful or realistic
- How could such a concept be realized? (states, supranational structures, UN, etc.)
- How relevant are the developments for a continuation of a truly global cyber society? (Internet as a global space vs Splinternet approach by nationally dividing platforms or providing nationally distinct regulation)
- What potential role might neutral countries or neutral platforms take in the international community? How should it be regulated (if at all) and who does it benefit? Drawbacks?

Appendix F

Interviews Conducted

As outlined in Chapter 1, the contents of interviews relevant for this thesis are included in the following sections of this appendix. The reader is reminded that most of the interview data is not provided as literal transcript but rather as notes taken during the interview and only minimally redacted. Some interview data is held in German, due to the language of the interviewee.

F.1 Interview 1

Confronted with the question whether Switzerland should perform *hack backs* and their opinion on neutrality in cyberspace:

As a state institution, we definitely should not do this. This is a question of ethics for me. Switzerland does not do that. I personally think that Switzerland should not shoot anywhere as it is a neutral country. This does not only count for the world of cyberspace. But that is my personal opinion. [...] As a country, we cannot provide a secure cyberspace for diplomats. Two years ago the nuclear negotiations with Iran were tapped in Western Switzerland. Kaspersky was compromised. No country could provide such a form of cybersecurity. We have virtually heard of this incident in the media. The correct path for Switzerland is to act in a neutral way. In times of war, the Federal Council could authorise the Department of Defence to “shoot back” by means of emergency law. Both the capacity and the knowledge are available from the Department of Defence. I think that neutrality is very important for our country. The example of terror attacks in Europe shows that it is probably due to our neutrality that we

have been spared. In the cyberdomain, however, we cannot find any difference in terms of attack intensity or attack frequency between ourselves and other countries. After all, the considerations there are mostly not about war but about economical reasons or data theft. I do not believe that Switzerland is in any way better off with regards to cyberspace than any other country. Neutrality does not have a direct positive effect there. I believe that neutrality generally does not play any important role in cyberspace, as we have not yet come across a situation where Switzerland had to act in a neutral way.

The interviewee further outlined the high importance of collaboration with supranational organisations. In particular, the collaboration with Western European countries within a format called “EGC” is of significant importance. For purists of a strict neutrality this collaboration might already be a sign of impartiality that could reduce trust in Switzerland. However, the collaboration is purely civilian and Switzerland does not have any obligations or allegiance with it. Finally, the interviewee emphasises that Switzerland should never try to *shoot back* or actively launch a counter attack, as this would not be compatible with Switzerland’s neutrality.

F.2 Interview 2

*Around 2012 the OSCE started a process of confidence-building measures in the cyberdomain. With this process, Switzerland has started to work on its foreign policy profile on the topic. We have currently defined three key areas: confidence-building measures for the prevention of conflicts, discussion on norms, rules and principles (which are not legally binding but establish expectations and lead to predictability) and capacity building. The international law is always superordinate in these processes and Switzerland has a strong interest that it is not only applied but also enforced. In the cyberdomain this is a bit more delicate. Countries such as China or Russia claim that cyber is so new and different from everything else that it requires novel principles of international law. Then there are countries like Switzerland who support the idea that there are already rules in place, such as the *ius ad bellum* or the *ius in bello*. They should be used in cyber space.*

The interviewee acknowledges that there are some difficulties with applying current international law in cyber space:

Particularly, the deniability in cyberspace makes it difficult to define counter measures or adequate responses as a response to attacks. These are legal problems. For example, in case Switzerland is attacked, as this was the case in the 2009 attack against the Department of Foreign Affairs, there is the question of what means we have in order for a reaction. The first question that always has to be resolved is, where an attack came from. In cyberspace, this is difficult to determine. The security and foreign policy goal of the Department of Foreign Affairs is to keep cyberspace free and secure. We want cyberspace to be used for peaceful goals and think that people should be able to access it in case they want to do that.

On the matter of confidence-building mechanisms:

It is also about definitions: What does cyber space mean for Russia, for Switzerland etc. We are currently exchanging a catalog of different terminologies, in order to understand how different countries define the term “cyberweapon”.

What means does Switzerland have in order to respond to cyberattacks:

We can of course contact countries of whom we think that they are the origin of a cyberattack. This can happen by collaboration of our embassies with local authorities, in order to determine the origin of an attack. I think that offensive capabilities are in any case a necessity for us. We differentiate three domains of Computer Network Operations (CNO): Computer Network Defense (CND), Computer Network Attacks (CNA) and Computer Network Espionage (CNE). Switzerland has always said that CND is a necessity. The other two domains have only become possible since the ratification of the new law on intelligence agencies. From this September onwards, we will have the possibility to actively take counter measures. For example, we could bring down a data centre in a foreign country in case this would be necessary. We are currently in the process of building up this capability. It is important that we also have this for deterrence. We can say: We have specific structures, specific capabilities and specific means. Please do not attack us! We are able to fight back. In case of a conflict, the limitations set by international law should always be respected: The principle of humanity, necessity, distinction, proportionality etc. These

principles are also valid in cyberspace. One of the problems is how to differentiate between military and civil infrastructure in cyberspace. There are often strong interdependencies. Is a data packet transmitted during a time of conflict civil or military? Switzerland has the following attitude towards this problem: If in doubt, the object should be protected from harm. An expert group of the UN, which has been working on such problems since 2004, is the UN Group of Governmental Experts (UNGGE). However, one has to be aware that this group merely publishes recommendations. What we are currently lacking is declarations from countries that state how they anticipate to apply international law. We currently work towards the UNGGE to be as inclusive as possible. At the moment, it consists of only 25 countries, who define their view on cyber-governance. That is a fundamental problem for us. Switzerland has an interest that these topics are discussed by the UN. There are also risks connected with this: Countries such as the “five eyes” could lose control. For Switzerland, however, it is difficult to support such an argument, as we want discussions to be as broadly supported as possible. The current processes are reaching their limits.

On the classification of a cyber incident:

Ultimately it is a political decision and evaluation to define an activity as a conflict or an attack or to state that we have the right to defend ourselves due to a specific constellation of facts. It is only at this point where Switzerland can say, whether its right to neutrality is actually applied.

F.3 Interview 3

On the importance of neutrality:

I understand your question on neutrality very well. For me, it is an additional question that one has to ask permanently, even beyond its narrow legal definition. Do we suddenly affect neutrality? Consequentially, we also ask ourselves in times of peace, whether we can exchange something with an institution or a country. It could suddenly also develop towards an advantage in case the country enters a conflict. This could be an IOC or a piece of code. We are only a hand full of people who think into this direction. These are topics that have not been discussed so far,

as the discussion has been focused on the technological problem. Now we have come to a point where we see that cyberdefence is not only about technology, but about humans, psychology, politics, communication, processes etc. [...] During a war or even permanently the problem is, to see what effect our actions have and which meaning this has. I, personally, think that a lot has yet to be done in this domain.

On the actual work that has to be done in cyberspace and problems that have to be considered:

It is about backtracking. Not about surveillance. In case we ever want to ask, who is to blame, we will need some proof. [...] On the one hand, we can control the availability of our systems and then there is the supervision of the content. But where is the line between these two? In the case of cryptography, is this question of content or of operation? Countries with a restrictive understanding of politics quickly reach the problem of controlling the semantics. At the moment, we do not do that in the western world. The question is, whether we can keep doing this. There are also events that demonstrate why we might want more control mechanisms, if we think of recent election campaigns. We should not accept that everybody can state anything, even the contrary of what is true. [...] Or in case people, institutions or states abuse the systems and cause permanent damage. In case we suddenly reach the next level of sabotage of war with cyber (I do not want to speak of cyber war but rather cyber in war) then the circumstances will change fundamentally. Then we shall see developments like in China or Iran, who have built an intranet for their own people, apart from the access to to the normal Internet. There could be the possibility of constructing an intranet, where misconduct is not tolerated and the borders between “do” and “do not” are very clear. In exchange, people can use a system which is secure and clear. We could then let the regular internet develop into any direction. These are questions of a strategic nature.

On what Switzerland is allowed to do in order to defend itself in cyberspace:

We have the Tallinn manual. This is, however, a purely western perspective of the problem. Other countries have a different perception of the problem. [...] We will have to rethink the principle of neutrality in any

case. We have to be careful: Neutrality was created in order to prevent Switzerland's participation in foreign wars. Neutrality does not have to become something that harms our own national interests. We have to be careful to not suddenly mix up law and ethics and moral. I think every country is allowed to take measures in order to defend itself. A case of espionage is, from my point of view, the easiest case. It is much more difficult in case of a fire and movement attack, where one is confronted with damage and has to stop an ongoing attack. You have to be absolutely sure, where the attack is coming from, before any counter measures can be taken.

On whether neutrality is important for Switzerland:

Security policy and neutrality are inherently connected with one another. Switzerland has been able to avoid a lot of big accidents thanks to neutrality. [...] I am convinced, that neutrality is not only a policy but also a culture. It is the DNA of our country, that we say we work well but we do not meddle in other's affairs. I think we can win far more with this attitude and the spirit of: "We want to help other find solutions for their conflicts". The question is, however, to which extent we can continue to do this in the cyber domain. [...] I am shocked to see that every time we encounter an incident we always talk about China, Iran, Russia or Northern Korea, yet the US and the Europeans cause a massive amount of incidents, in particular the United Kingdom, who has attacked Belgium, and do not take any harm from it. They always point their fingers to the others. I think that Switzerland could play an important role as a neutral expert in establishing a certain sense of morale.

F.4 Interview 4

Neutralität ist auch im Cyberspace wichtig. Krieg im Cyber Space ist ein relativ neues Phänomen. Seit Stuxnet im Iran ist es ins Bewusstsein gekommen. Man merkt erst, dass es eine Form der Auseinandersetzung zwischen Ländern ist. Ansonsten haben Länder ja das internationale Kriegsvölkerrecht. Es gibt aber für Cyber-Law kein solches Centre, jedenfalls international gesehen. Man könnte bspw. In Genf ein solches Center gründen für Cyber-Neutralität.

Über die Wichtigkeit des Standorts Schweiz: Fast ein Viertel des europäischen Datenvolumens wird in der Schweiz gespeichert. Tendenz steigend. Mehr als 1Mrd Franken wurde in den Bau von Data Centres gesteckt. Neutralität ist auch ein Wirtschafts- und Standortfaktor. Firmen suchen Standort wo man geschützt ist, wo die Daten beherbergt sind. Wenn ein Land Ziel sein kann ist das ein Risikofaktor.

Über die Werte der traditionellen schweizer Neutralität: Wieso kommen Kunden in die Schweiz? Der Überbegriff ist Stabilität. Wenn man weiter geht, dann fängt das an mit:

- Gute Infrastruktur, bspw. Stromversorgung;
- stabile politische Verhältnisse;
- hohe Verlässlichkeit: stabiler Arbeitsmarkt, keine Aufstände;
- gute Fachleute und gute Ausbildung.

Betreffend Kapazitäten: Die Schweiz ist von dieser Thematik zu Cyber / Überwachung / Sicherheit völlig überrascht worden. Wir sind nicht vorbereitet. Es kommt langsam ein wenig Bewegung in die Sache. Aber wir sind blind auf beiden Augen. Verfassungsmässig (Art. 13): Der Staat nimmt als Kernaufgabe die Sicherheit wahr. Der Staat hat eine hoheitliche Aufgabe, welche bisher mit einer klassischen Armee gelöst wurde (wahrscheinlich auch in Zukunft) aber auch neue Bedrohungen aus dem Cyber-Raum kommen hinzu. Beispiele: Fall RUAG, 18 Monate hat niemand etwas gemerkt. Ausländische Nachrichtendienste mussten uns informieren.

Internationale Kooperation: Man könnte sagen Es gibt keine Territorialgrenzen im Cyberspace. Es hätte aber sein können, dass uns ausländische Dienste gar nicht informiert hätten! Jedes Land muss sich selbst schützen können, ein Lagebild machen etc. Sicher sich selbst und kritische Infrastruktur schützen können. Was der Staat nicht kann ist: Unternehmen schützen.

Zusammenarbeit mit anderen Staaten: Heute beschäftigen sich Polizeikorps mit dem Thema. Zusammenarbeit ist gut und wünschenswert. Im Bereich der Nachrichtendienste funktioniert die Zusammenarbeit auch gut mit befreundeten Ländern: DE, ISL, FR: Diese haben aber stets neben Nachrichtendienst und Polizei eine eigene Cyber-Abwehr. Motto DE: so wie im Luftraum gibt es auch einen Cyber-Raum. DE haben ein Cyber-Kommando mit Cyber-Kommandeur (gleiche Stufe wie LW). Es gibt dennoch Aufgaben wo man selber agieren muss. Zusammenarbeit muss aber mit Sicherheit funktionieren. Das Schneidet sich meines Erachtens auch nicht mit der

Neutralität.

Zur NATO-Orientierung: Tatsächlich ist dies eine Gefahr. Die NATO hat aber auch nicht mehr denselben Stellenwert. Insbesondere jetzt unter Donald Trump: man kann sich nicht auf die Amis verlassen. Die Länder müssen Zepter wieder mehr selbst in die Hand nehmen. CH tut gut daran, nicht nur neutralitätspolitisch, sondern auch unabhängig die Sicherheit zu gewährleisten.

F.5 Interview 5

Zu einem Beitrag von neutralen Akteuren im Cyber-Raum:

- Anwendbarkeit von Neutralitätsrecht in Konfliktsituation. Wann kann man von einer Kriegshandlung sprechen? Diese Frage ist sehr wichtig, denn Neutralitätsrecht ist gebunden an Konfliktsituation. UN Art. 51 erlaubt "self defence". Also wann findet ein Angriff statt im Cybr-Raum? Die Konfliktaustragung ist nicht auf Cybr-Raum beschränkt. Wo ist diese Kriegsschwelle?
- USA beantworten dies, wenn dem UN-Sicherheitsrat mitgeteilt wird, dass es sich um eine Kriegshandlung handelt. Denn das kann sehr einfach eskalieren. UN-Sicherheitsrat setzt diese Schwelle hoch an: Nur bei einem massiven physischen Schaden. (bspw. Staudämme die zum Einsturz gebracht werden). Das muss geklärt sein. Man sagt einfach das Neutralitätsrecht ist einfach im Cybr-Raum auch anwendbar. Das ist ungenügend.
- Das zweite ist die Neutralitätspolitik: Verhalten, das es glaubwürdig macht, dass man neutral ist, auch im Konfliktfall. Vertrauensbildende Massnahmen, verkraftbare Formen der Zusammenarbeit, damit die Neutralität glaubwürdig bleibt. Heikle Frage: Was verlangt die UNO damit man einem angegriffenen Staat im Cybr-Raum Hilfe leistet?
- Das dritte: was kann ein Neutraler Staat machen, um einen freidlichen Cyber-Raum zu fördern? Die traditionellen Mittel der guten Dienste sind hier schwierig. Bei der Abklärung von Tatsachen -> ähnlich wie das Labor Spiez. Also Transparenz über Ursprünge herstellt. Dialog-Plattformen zur Verfügung stellen, da wir nicht Teil eines Machtblockes sind. Das kann nicht jedes Land in dieser Form machen, das setzt auch ein gewisses Know-How voraus.

- Rückmeldungen zu den Papers: Drei Typen der Cyber Operationen. CNA, CNE, information operations (via soziale Medien). Für den Völkerrechtler ist nur CNA relevant. CNE ist keine Verletzung der Neutralität, Information Operations sind auch keine Verletzung der Neutralität. Das Problem wäre ja sonst, dass Fehlinformationen dann als Kriegshandlung gesehen werden können.
- Es geht ja schlussendlich um eine Handlung: die Frage ist dann, wie wird das definiert? Im spezifischen Fall ist es ja dann ein Unterschied. Es heisst nicht, dass da alles zulässig sein soll! Denn da gibt es auch Konzepte für responsible behaviour. Es ist zwar kein Fall für Kriegshandlung aber trotzdem eine Gefahr. Es braucht Regeln aber es ist keine Frage des Neutralitätsrechts.
- Plattform-Neutralität: Es geht eigentlich um eine Art Thematik, die auch bei Network-Neutralität existiert. Unabhängig der Quelle soll jemand den Inhalt verbreiten können. Auch gewisse ethische Normen die einzuhalten sind, Guvernanz-Fragen (wer soll das regeln) und auch inhaltlich wer das machen soll. Es kann aber wahrscheinlich nicht einfach durch eine "Haager Konvention" beschlossen und festgelegt werden, sondern es würden vielleicht Verhandlungen nötig sein. Mann will nicht destabilisieren, Hass oder Konflikt, fördern, aber man möchte auch nicht, dass die Meinungsäusserungsfreiheit Schaden nimmt. Das Problem ist dann auch wenn es Beziehungen zur anderen Partei gibt und wo es Parteispenden gibt zu den Demokraten.
- Die Frage ist, ob die Anlehnung an die Neutralität möglich ist, oder ob man nicht eher einen Kodex finden sollte: Ist die Transparenz verpflichtend? Vielleicht der Verzicht auf Einsatz von Bots (Meinungsbeeinflussung), eine vernünftige Balance finden zwischen Anonymität und Schutz der Privatsphäre (Problem: Länder mit autoritären Strukturen). Neutralität würde in so einer Optik nicht dasselbe bedeuten wie in einem Konflikt zwischen Staaten, sondern dass man sich inhaltlich zurückhält und nicht die ganze Macht die man hat einsetzt.
- Nach Peking und nach Moskau schauen: dort ist vor allem der Ansatz, dass man das Internet fragmentieren möchte. ("Information Security"). In Russland besteht Kontrolle über Infrastruktur und Inhalte, was ein Problem ist. Das würde die Offenheit des Internets zerstören. Das Problem ist in der UN, dass die Key Player sich nirgends festlegen möchten (USA, China, etc.) Darum ist der Weg zu einem Code of Conduct zu kommen (rechtlich nicht bindende Absprachen) wo man Regierungen und Technologiekonzerne mit einbeziehen

kann. Die grossen Tech-Konzerne wissen dass es irgendwann ein Problem gibt mit Staaten, wenn sie einfach nur ihren Businessplan verfolgen. Da benötigt es einen Prozess der Diskussion. Also ein innovatives Vorgehen um Probleme zu lösen, auszuwerten, Best practices finden etc. Also wahrscheinlich keine internationale Konvention als Lösung, die das regeln könnte.

- Es ist neuartig, weil private Akteure dabei eine enorme Rolle spielen! Das war früher nicht so. Es konnte nicht jeder ein Atom-U-Boot bauen etc. Nun ist es aber so. Auch der Einstieg in diesen Bereich ist sehr niederschwellig! Gruppen die eindringen in Systeme, das gibt es in dieser Form in der kinetischen Welt weniger. Klar gibt es Guerillas, aber das ist ganz anders! Dies ist ähnlich wie Staaten.

F.6 Interview 6

No relevant input for the topic of this thesis from interview.

F.7 Interview 7

Was ist der Unterschied im Cyber-Bereich und im anderen Bereich? Die Grundprinzipien sind wohl ähnlich und es geht bloss darum, dass man im Cyber-Bereich sich ähnlich verhält. Wichtiger Aspekt: Es gibt Staaten die in dem Bereich aktiv sind, da ist es nötig, dass man neutral bleibt. Es gibt viel deniability: es ist schwierig nachzuweisen. Gerade dort kann ein neutraler Akteur sehr wichtig sein. Im Bereich relative Neutralität gibt es viele rechtliche Fragezeichen. Ein Problem als parallele: Überflugsrechte. Cyber-Bereich: Schritte die vorsehen, dass Leitungen nicht benutzt werden. Momentan ist dies nicht möglich. Es gibt da Fragezeichen.

Tallinn ist ein akademisches manual: die sagen alle ganz klar, das ist ein Experten-Dokument. Es ist nicht Staaten-Werk. Viele Staaten haben eigene Operationen / Abläufe.

Zu Toolkits bzw. multilateralen Werkzeugen und Normen:

Cyber Law Toolkit: Staatenpositionen sind da. Rund 20 Positionen sind da, evtl können die sogar nach Thematik sortiert werden. Schweiz ist dort, Niederlande, etc. Aspekte der rechtlichen Neutralität sind dort.

OEWG: Da sitzen alle Staaten, mit Experten, Diplomaten, etc. Grosse Linien werden da abgehandelt. Da spricht dann jeder Staat so 5 Minuten, die Details werden nicht besprochen, insb. Die Frage der Neutralität wird nicht angesprochen.

UN GGE: waren 25 Länder, vor allem Experten, Diskussionen hinter verschlossenen Türen. Da gingen Diskussionen wohl in grössere Details. Reports erwähnen Neutralität nicht. Ne grosse Debatte ist, ob das humanitäre Völkerrecht anwendbar ist. Neutralität kommt da nicht rein.

Neutraler Staat: darf Spionage betreiben? Spionage könnte Teil sein eines breiteren Angriffes sein. Reconnaissance-Phase eines Angriffes? Spionage wird als völkerrechtlich unproblematisch angesehen, weil es jeder macht.

Anforderung: Medizinische Akteure müssen respektiert und geschützt werden: kein Schaden zufügen. Was bedeutet das in Bezug auf Spionage? Sicherstellen, dass IKRK zB wirklich auch IKRK ist: so muss es Verifizierungen geben können. Der Unterschied muss gemacht werden: Krankenhaus muss überprüft werden, zB auch die Computer. Spionage ist trotzdem legitim (auch gegen IKRK).

Nachrichtendienstliche Arbeit oder militärische Zusammenarbeit? Nur Informationsaustausch ist eine Sache, wenn Information operationell relevant ist, dann wird das nicht mehr neutral. Wenn die Schweiz Surveillance in Syrien machen würde und dann Standorte an USA weitergibt von ISIS Truppen. Vulnerabilities dürfen nicht weitergegeben werden im Cyber-Raum. Es gibt Kriterien die das unterscheidbar machen. Staatliche Neutralität: Yes there is a benefit! Beispiel ist die schweizer Rolle im Iran. Wenn Staaten nicht sprechen zusammen, dann ist Eskalation absehbar. Im Cyber-Bereich ist viel Misstrauen und Deniability, deswegen ist Dialog essentiell. Ein neutraler Staat kann eine wichtige Rolle spielen. Ein neutraler Staat der Services anbieten kann kann ist wichtig. Eine Attribution Agency wäre wichtig. Attribution ist nicht unmöglich. Der Punkt ist, dass sie oft nicht wirklich beweisen können, da sie nicht genau sagen können wieso sie wissen woher es ist (Intel Assets würden preisgegeben werden.).

Staaten haben den Eindruck dass sie handeln können, da sie nicht zur Rechenschaft gezogen werden können. Problem ist mit Agency: Würde der neutrale Staat als solcher akzeptiert? Da gebe es wohl politisches Gegensteuern gegen die Berichte etc. Big Tech Companies are being perceived as actors. Microsoft hat eine diplomatische Vertretung sowohl in Genf als auch New York für Cyber Diplomacy. Die werden als Akteure wahrgenommen. Nicht als den Staaten gleich aber als wichtiger Akteur. Im Social-Media-Bereich sehen viele eine wichtige Rolle der Social-Media-Company. Die Blicke richten sich viel auf diese Companies. Es wird mit Microsoft, Facebook und Twitter gesprochen. Einfluss und Wichtigkeit wird anerkannt. Es würde wohl einen Dialog geben, im Falle von operationell relevanten Hass-Nachrichten.

Problematisch: Die Companies sind alle im Silicon Valley aus den USA. Die werden

als aus den USA wahrgenommen. Sie verhalten sich nicht neutral. Konversationen: einige Companies haben Stellung bezogen, zB beim Arab Spring wie auch bei den Riots beim Capitol. Die Aktivitäten sind ja nicht unbedingt eine neutrale Haltung. Viele Companies werden als verlängerter Arm der US-Aussenpolitik gesehen.

Man muss nicht neutral in Bezug auf Menschenrechtsverletzungen sein. Vorwurf ist die fehlende Unabhängigkeit vom amerikanischen Staat. Das stellt die Neutralität in Frage. Die Frage der Perception of Independence / Neutrality / Impartiality sich verändert hat als Donald Trump auf Social Media eingeschränkt wurde.

Schutz von telekom-Infrastruktur und Social media: Rechtliche Grundlage: Distinction bedeutet, dass nur militärische Ziele angegriffen werden dürfen. Zivile Objekte dürfen nicht angegriffen werden, können aber zu Zielen werden, wenn diese Infrastruktur zum Beispiel militärisch genutzt wird. Telekom-Infrastruktur, die militärisch genutzt werden kann, kann zum Ziel werden. Darf nicht disproportional sein. Militärischer Vorteil muss grösser sein als Leid das der zivilen Bevölkerung.

F.8 Interview 8

Zu staatlicher Neutralität: Völkerrechtliches Prinzip der Neutralität. Im Cyberraum ist die Problematik dass sich das nicht mehr trennen lässt zwischen innen und aussen: wie lässt sich das vereinbaren? Nach aussen neutral kann nach innen Implikationen nach sich ziehen. Also Passivität? Wo passiert Cyber-Abwehr? Also ein neutraler Staat sollte gar nichts durchführen. Neutralität war früher immer Territorial. Da fehlt ein wenig das Interesse. Wir wissen noch nicht genau wann ein Angriff ein Angriff ist, das ist noch nicht so klar bei Cyber. Wir sind momentan im "Unfrieden". Als neutraler Staat ist mein Ziel zumindest den Unfriedens-Zustand zu bewahren und keinerlei Angriffe zuzulassen.

Zu Platform Neutrality: Es geht um die Beziehung Staat-Konzerne:

Grosse Unternehmen: sind immer getrieben von finanziellen Interessen. In diesem Sinne sind sie gar nicht neutral. Es gibt keine Regulierung durch die Staatengemeinschaft. Die grossen Gatekeeper haben fast eine überstaatliche Position. Sie können unabhängig von Vertragsstrukturen agieren. Unternehmen als Teil des anarchic system of states. Recht kommt nicht wirklich weit und Territorial kommt man auch nicht weit. Beispiel Telegram in Deutschland.

Status quo: die wirtschaftlichen Interessen sind derart gross, dass sie überhand nehmen. Die Interessen sind bei Staaten derart vielschichtig, dass man das nicht vergleichen kann—zwar hat ein Staat wirtschaftliche Interessen, aber nicht nur. Die

Plattformen treibt hauptsächlich dieses Interesse an. Das Problem ist der Algorithmus in diesem Rahmen: der status quo in diesem Fall ist nicht so. Die bisherigen Plattformen, in dem Sinne, historisch, in den Anfangsphasen und so weiter, stellen die Glaubwürdigkeit in Frage etc. Die Algorithmen-Themen sind da auch ein riesiges Problem.

Oversight Board: Legitimation durch Verfahren. Wie werden Menschen gewählt? Wie funktionieren die Verfahren? Veranstaltung Hass und Hetze: von der KAS. Anwältin von Facebook hat erklärt wie die Prozesse ablaufen.

DSA: das ist ein Köder um aus dem Dialog ne Regulierungsbasis zu schaffen. Man muss sie ja irgendwie an den Tisch kriegen. Auch EU-weit hilft es; weil da Standards für viele Länder gesetzt werden. Klarnamen-Diskussion bringt nicht so viel.

Platform Neutrality und Strukturen: das wäre absolut hilfreich und wünschenswert. Wir brauchen einen Moderator für sowas. Es braucht eine Rechtssicherheit und ein Vertrauen in die Rechtssicherheit. Also es muss vielleicht sogar über supranational sein. Also China und Russland schaffen sich auch abzuschotten. Also vielleicht alle die daran partizipieren und so werden von was UN-mässigem gemonitored. A moderator function is needed! Wer kann Moderator sein? UN-Organisation mit Unternehmen die völkerrechtlichen Status haben? Problem: Völkerrecht ist ein relativ stumpfes schwert das selektiv angewendet wird. Idealvorstellung: Institution die sich auf Gemeinnützigkeit und Allerweltsnutzen versteift. Dieses Unternehmen braucht einen Checks and Balance Mechanismus. Ansatz wie das rote Kreuz? Oder neutraler Staat?

Bibliography

- [1] A. S. Tanenbaum and H. Bos, *Modern Operating Systems*, 4th ed. New Jersey: Pearson Education, 2014, vol. 2.
- [2] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Boston: Pearson Education, 2011.
- [3] M. Stolz, “Competing Interests of Cyberintelligence and Cyberdefence Activities in Neutral Countries 3 . Conceptualisation of Operations in Cyberspace,” in *16th International Conference on Cyber Warfare and Security*. Online: ACI, UK, 2021, pp. 345–353.
- [4] N. Neuman, “Neutrality and Cyberspace: Bridging the Gap between Theory and Reality Neutrality and Cyberspace: Bridging the Gap between Theory and Reality,” *International Law Studies*, vol. 97, pp. 765–802, 2021.
- [5] A. Riklin, *Funktionen der schweizerischen Neutralität*. St. Gallen: Institut für Politikwissenschaft, Universität St Gallen, 1991.
- [6] GovCERT.ch, “APT Case RUAG Technical Report,” Swiss Confederation, Tech. Rep. 2016-05-23, 2016.
- [7] J. P. Barlow, “A Declaration of the Independence of Cyberspace,” 1996. [Online]. Available: <https://www.eff.org/de/cyberspace-independence>
- [8] L. Kello, *The Virtual Weapon and International Order*. New Haven: Yale University Press, 2017.
- [9] T. Wu, “Network Neutrality, Broadband Discrimination,” *Journal on telecommunications & high technology law*, vol. 2, no. 1, p. 141, 2003.
- [10] M. Jorio, “Die Neutralität – aktiv, differenziell oder kooperativ?” Zurich, 7 2022. [Online]. Available: <https://www.nzz.ch/meinung/babylonisches-sprachengewirr-um-die-neutralitaet-ld.1693051>

- [11] S. Caminada, “"Arena" zur Neutralität - Bankenvertreter liefern sich Duell um Oligarchengelder - News - SRF,” 2023. [Online]. Available: <https://www.srf.ch/news/schweiz/arena-zur-neutralitaet-bankenvertreter-liefern-sich-duell-um-oligarchengelder>
- [12] A. Spring, *The International Law Concept of Neutrality in the 21st Century. An Analysis of Contemporary Neutrality with a Focus on Switzerland*. Zürich / St. Gallen: Dike, 2014.
- [13] M. Tedre, *The Science of Computing: Shaping a Discipline*. London: Chapman and Hall/CRC, 2014.
- [14] N. Angius, G. Primiero, and R. Turner, “The Philosophy of Computer Science,” Stanford, 1 2021. [Online]. Available: <https://plato.stanford.edu/entries/computer-science/>
- [15] O. U. Press, “About | Journal of Cybersecurity | Oxford Academic,” 2023. [Online]. Available: <https://academic.oup.com/cybersecurity/pages/about>
- [16] Oxford University Press, Ed., *Oxford English Dictionary*. Oxford: Oxford University Press, 2018. [Online]. Available: <https://www.oed.com>
- [17] G. Kreis, “Neutralität und Neutralitäten,” in *Die Geschichte der Schweiz*, G. Kreis, Ed. Basel: Schwabe Verlage, 2014, pp. 306–309.
- [18] J. S. Nye and D. A. Welch, *Understanding global conflict and cooperation : an introduction to theory and history*, 10th ed. Boston: Pearson, 2017.
- [19] A. Heywood, *Global Politics*, 2nd ed., ser. Palgrave foundations. Basingstoke: Palgrave Macmillan, 2014.
- [20] Theucydides, *History of the Peloponnesian War*. Greece: Ancient, -400.
- [21] Thucydides, M. Hammond, and P. J. Rhodes, *The Peloponnesian War*, ser. Oxford world’s classics. Oxford: Oxford University Press, 2021.
- [22] C. K. Lamont and M. M. Boduszynski, *Research Methods in Politics and International Relations*. Los Angeles: SAGE PUBLICATIONS, 2020.
- [23] R. K.Yin, *Case study research and applications: Design and methods*, 6th ed. Los Angeles: SAGE PUBLICATIONS, 2018.

- [24] J. Hills, *The Struggle for Control of Global Communication: The Formative Century*, ser. History of communication. Urbana: University of Illinois Press, 2002.
- [25] —, *Telecommunications and Empire*. Urbana: University of Illinois Press, 2007.
- [26] B. Buchanan, *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press, 2017.
- [27] M. N. Schmitt, Ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 3 2013. [Online]. Available: <https://www.cambridge.org/core/product/identifier/9781139169288/type/book>
- [28] —, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2 2017. [Online]. Available: <https://www.cambridge.org/core/product/identifier/9781316822524/type/book>
- [29] IEEE Periodicals, “IEEE REFERENCE GUIDE,” IEEE, Piscataway, NJ, Tech. Rep., 2018. [Online]. Available: <https://ieeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf>
- [30] Victoria University, “Overview - IEEE Referencing - Library Guides at Victoria University,” 2023. [Online]. Available: <https://libraryguides.vu.edu.au/ieeereferencing>
- [31] E. Egli, A. Diem, T. Maissen, and D. Wachter, “Switzerland,” London, 2023. [Online]. Available: <https://www.britannica.com/place/Switzerland>
- [32] The Information Architects of Encyclopaedia Britannica, “Switzerland Facts,” 2023. [Online]. Available: <https://www.britannica.com/facts/Switzerland>
- [33] Federal Chancellery, “The Swiss Confederation. A brief guide. ,” Swiss Confederation, Bern, Tech. Rep., 2022. [Online]. Available: <https://www.ch-info.swiss/edition-2022/edition-2022/deckblatt-ausgabe-2022>
- [34] Federal Department of Defence, “Die Neutralität der Schweiz,” 2000. [Online]. Available: <https://www.parlament.ch/centers/documents/de/armee-21-neutralitaet-d.pdf>

- [35] —, “Swiss Neutrality,” 2004. [Online]. Available: <https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/Swissneutrality.pdf>
- [36] Federal Department of Foreign Affairs FDFA, “Neutrality,” 2017. [Online]. Available: <https://www.eda.admin.ch/eda/en/home/foreign-policy/international-law/neutrality.html>
- [37] A. Suter, “Neutralität. Prinzip, Praxis und Geschichtsbewußtsein.” in *Eine kleine Geschichte der Schweiz*. Frankfurt (Main): Suhrkamp, 1998, pp. 133–188.
- [38] M. Hettling, M. Schaffner, and M. König, Eds., *Eine kleine Geschichte der Schweiz*. Frankfurt (Main): Suhrkamp, 1998.
- [39] T. Szvircsev Tresch, S. De Rosa, T. Ferst, P. Rohr, and J. Robert Bericht vom, “Nachbefragung der Studie "Sicherheit 2022" aufgrund des Krieges in der Ukraine Aussen-, Sicherheits-und Verteidigungspolitische Meinungsbildung im Trend,” ETH Zurich, Zurich, Tech. Rep., 7 2022. [Online]. Available: <https://www.newsd.admin.ch/newsd/message/attachments/72460.pdf>
- [40] S. Cordey and K. Kohler, “The Law of Neutrality in Cyberspace,” Centre for Security Studies, ETH Zurich, Zurich, Tech. Rep., 12 2021.
- [41] M. Dahinden, “Swiss neutrality in the age of cyber warfare: discussion paper,” ICT4Peace, Geneva, Tech. Rep., 2021. [Online]. Available: www.zora.uzh.ch/year:2021URL:https://doi.org/10.5167/uzh-211055
- [42] J. Latson, “Swiss Neutrality Doesn’t Mean Pacificism: How Switzerland Got That Way | Time,” 2015. [Online]. Available: <http://time.com/3695334/switzerland-neutrality-history/>
- [43] M. Stolz, “On Neutrality and Cyber Defence,” in *18th European Conference on Cyber Warfare and Security*, T. Cruz and P. Simoes, Eds. Coimbra: ACPI, UK, 2019, pp. 484–491. [Online]. Available: <https://ora.ox.ac.uk/objects/uuid:9f1a1f50-2e9a-40c5-84fe-309da52dbab4>
- [44] F. Egloff, “Cybersecurity and the Age of Privateering,” in *Understanding Cyber Conflict: Fourteen Analogies*, G. Perkovich and A. E. Levite, Eds. Georgetown University Press, 2017, ch. 14.
- [45] T. Hobbes, *Leviathan*. London: Andrew Crooke, 1651.

- [46] J. S. Nye, *The Future of Power*, 1st ed., ser. Ebook central. New York: PublicAffairs, 2011.
- [47] C. L. Glaser and C. Kaufmann, “What Is the Offense-Defense Balance and Can We Measure It?” *International Security*, vol. 22, no. 4, pp. 44–82, 1998. [Online]. Available: <https://www.mitpressjournals.org/doi/pdf/10.1162/isec.22.4.44>
- [48] F. J. Egloff, “Contested public attributions of cyber incidents and the role of academia,” *Contemporary Security Policy*, vol. 41, no. 1, pp. 55–81, 1 2020. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/13523260.2019.1677324>
- [49] T. Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, vol. 35, no. 1, pp. 5–32, 2012. [Online]. Available: <http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939>
- [50] E. Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” *International security*, vol. 38, no. 2, pp. 41–73, 2013.
- [51] L. De Mol, “Turing Machines,” Stanford, 9 2018. [Online]. Available: <https://plato.stanford.edu/entries/turing-machine/>
- [52] Schweizer Armee, “Taktische Führung 17 Kapitel 7 – Verteidigung,” Schweizerische Eidgenossenschaft, Tech. Rep., 2019.
- [53] US Department of Defense, “The National Military Strategy for Cyberspace Operations,” US Department of Defence, Washington D. C., Tech. Rep., 2006. [Online]. Available: <http://www.bits.de/NRANEU/others/strategy/07-F-2105doc1.pdf>
- [54] The Hague Convention, “Rights and Duties of Neutral Powers and Persons in War on Land,” *The Hague Convention*, vol. V, 1907.
- [55] —, “Rights and Duties of Neutral Powers in Naval War,” *The Hague Convention*, vol. XIII, 1907.
- [56] The Geneva Conventions, “Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field,” *The Geneva Conventions*, vol. I, 1949.

- [57] —, “Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea,” *The Geneva Conventions*, vol. II, 1949.
- [58] —, “Convention (III) relative to the Treatment of Prisoners of War,” *The Geneva Conventions*, vol. III, 1949.
- [59] —, “Convention (IV) relative to the Protection of Civilian Persons in Time of War,” *The Geneva Conventions*, vol. IV, 1949.
- [60] —, “Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I),” *The Geneva Conventions*, vol. I, 1977.
- [61] —, “Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II),” *The Geneva Conventions*, vol. II, 1977.
- [62] —, “Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III),” *The Geneva Conventions*, vol. III, 2005.
- [63] ICRC, “Customary law.” [Online]. Available: <https://www.icrc.org/en/war-and-law/treaties-customary-law/customary-law>
- [64] J. Silomon, “Software as a Weapon: Concepts, Perceptions, and Motivations in Pursuit of a New Technology of Conflict,” 2021.
- [65] J. E. Kastenber, “Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law,” *Air Force Law Review*, vol. 64, 2009. [Online]. Available: https://digitalrepository.unm.edu/law_facultyscholarship/436
- [66] W. H. von Heinegg, “Neutrality in Cyberspace,” *International Conference on Cyber Conflict (CyCon)*, vol. 4, pp. 35–46, 2012. [Online]. Available: <http://www.icrc.org>.
- [67] —, “Territorial Sovereignty and Neutrality in Cyberspace,” *International Law Studies*, vol. 89, pp. 123–156, 2013.

- [68] Cloudflare, “What is a WAF? Web Application Firewall explained.” [Online]. Available: <https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>
- [69] V. Sundar, “How Does WAF (Web Application Firewall) Works?” 3 2019. [Online]. Available: <https://www.indusface.com/blog/how-web-application-firewall-works/>
- [70] A. Holenstein, *Mitten in Europa. Verflechtung und Abgrenzung in der Schweizer Geschichte*. Baden: Hier und Jetzt, 2014.
- [71] G. Kreis, Ed., *Die Schweizer Neutralität : beibehalten, umgestalten oder doch abschaffen?* Zürich: Werd-Verlag, 2007.
- [72] —, *Die Geschichte der Schweiz*. Basel: Schwabe Verlag, 2014.
- [73] International Committee of the Red Cross, “History of the ICRC,” 10 2016. [Online]. Available: <https://www.icrc.org/en/document/history-icrc>
- [74] S. Bradley, “From the League to the UN: ending Swiss isolationism,” Bern, 7 2019. [Online]. Available: https://www.swissinfo.ch/eng/politics/100-years-of-multilateralism_from-the-league-to-the-un--ending-swiss-isolationism/45106026
- [75] F. Burnand, “Switzerland, the League of Nations, and the shadow of revolution,” Bern, 7 2019. [Online]. Available: https://www.swissinfo.ch/eng/politics/100-years-ago_switzerland--the-league-of-nations--and-the-shadow-of-revolution/45081906
- [76] Dodis.ch, “The Establishment of Swiss Diplomatic Relations with the USSR,” Bern. [Online]. Available: <https://www.dodis.ch/en/establishment-swiss-diplomatic-relations-ussr#>
- [77] Federal Department of Foreign Affairs, “Former Cuban Interests Section,” 11 2017. [Online]. Available: <https://www.eda.admin.ch/countries/usa/en/home/representations/embassy-washington/embassy-tasks/cuba.html>
- [78] —, “Embassy of Switzerland - Foreign Interests Section,” 6 2022. [Online]. Available: <https://www.eda.admin.ch/countries/iran/en/home/representations/embassy/embassy-of-switzerland-foreign-interests-section.html>

- [79] The Swiss Armed Forces, “NNSC.” [Online]. Available: <https://www.vtg.admin.ch/en/aktuell/einsaetze-und-operationen/militaerische-friedensfoerderung/missionen/nns.html#ui-collapse-103>
- [80] F. Fukuyama, *The end of history and the last man*. London: Penguin, 1992.
- [81] M. Stolz, “On Neutrality and Cyber Defence,” Ph.D. dissertation, University of Oxford, 2017.
- [82] NZZ.ch, “Calmy-Reys Interpretation der Neutralität,” Zurich, 11 2003. [Online]. Available: <https://www.nzz.ch/article987SR-ld.278984>
- [83] —, “Neutralitätsrhetorik und Sendungsgedanken,” Zurich, 2 2005. [Online]. Available: <https://www.nzz.ch/kommentarCKUKN-ld.332290>
- [84] —, “Neutralität - ein Verbrechen?” 2 2005. [Online]. Available: <https://www.nzz.ch/articleCL9OA-ld.332555>
- [85] —, “Den aussenpolitischen Kompass ausrichten,” Zurich, 5 2005. [Online]. Available: <https://www.nzz.ch/articleCT501-ld.344463>
- [86] —, “Mangelnde Kohärenz in der Aussenpolitik,” Zurich, 5 2005. [Online]. Available: <https://www.nzz.ch/kommentarCTTF3-ld.345180>
- [87] —, “Erweiterung der aussenpolitischen Pupillen,” 5 2005. [Online]. Available: <https://www.nzz.ch/articleCTWXZ-ld.345177>
- [88] —, “Calmy-Rey will weg von der EU-Fixierung,” Zurich, 5 2005. [Online]. Available: <https://www.nzz.ch/articleCTPRQ-ld.345426>
- [89] —, “Erwartungen an die schweizerische Aussenpolitik,” Zurich, 6 2005. [Online]. Available: <https://www.nzz.ch/articleCUMDD-ld.346830>
- [90] —, “Aktive Neutralitätspolitik als Interessenpolitik,” Zurich, 11 2005. [Online]. Available: <https://www.nzz.ch/articleDB8LQ-ld.367405>
- [91] C. Raaffaub and F. Brunand, “"Die aktive Neutralität ist nichts Neues",” 8 2006. [Online]. Available: <https://www.swissinfo.ch/ger/-die-aktive-neutralitaet-ist-nichts-neues-/5355986>
- [92] NZZ.ch, “Die Schweiz bald im Sicherheitsrat der Uno?” Zurich, 8 2006. [Online]. Available: <https://www.nzz.ch/articleEEJSR-ld.78861>

- [93] —, “Plädoyer für eine noch aktivere Aussenpolitik,” Zurich, 8 2006. [Online]. Available: <https://www.nzz.ch/articleEEITM-ld.75132>
- [94] R. Blatter, “Calmy-Reys "aktive Neutralität",” Zurich, 9 2006. [Online]. Available: <https://www.nzz.ch/articleEEOIH-ld.374880>
- [95] NZZ.ch, “SVP fordert Rückkehr zur passiven Neutralität,” Zurich, 1 2007. [Online]. Available: <https://www.nzz.ch/articleETW72-ld.393133>
- [96] —, “Schweiz als ehrlicher Broker,” Zurich, 6 2007. [Online]. Available: <https://www.nzz.ch/newzzf3i8kxyk-12-ld.416945>
- [97] —, “Calmy-Rey liebäugelt mit einem Sitz im Uno-Sicherheitsrat,” Zurich, 9 2007. [Online]. Available: https://www.nzz.ch/calmy-rey_liebaeugelt_mit_einem_sitz_im_uno-sicherheitsrat-ld.432257
- [98] —, “Sitz im Sicherheitsrat als Ziel,” Zurich, 9 2007. [Online]. Available: https://www.nzz.ch/sitz_im_sicherheitsrat_als_ziel-ld.432368
- [99] —, “Sicherheitsrat-Pläne stossen auf Ablehnung,” Zurich, 10 2007. [Online]. Available: https://www.nzz.ch/sicherheitsrat-plaene_stossen_auf_ablehnung-ld.437389
- [100] M. Furrer, “Angriff auf Calmy-Reys Erbe,” Bern, 9 2011. [Online]. Available: <https://www.derbund.ch/angriff-auf-calmy-reys-erbe-436162884363>
- [101] H. Mooser, “Das war die Ära Calmy-Rey,” Bern, 12 2011. [Online]. Available: <https://www.derbund.ch/das-war-die-aera-calmy-rey-890937054269>
- [102] Federal Council, “Standortbestimmung des Bundesrats im Ukraine-Konflikt,” Swiss Confederation, Bern, Tech. Rep., 3 2014. [Online]. Available: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-52440.html>
- [103] —, “Situation in der Ukraine: Bundesrat weitet seine Politik zur Vermeidung von Umgehungen aus,” Swiss Confederation, Bern, Tech. Rep., 8 2014. [Online]. Available: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-54069.html>

- [104] S. Bondolfi and K. Dhif, “"Die Schweiz und ihre Neutralität stehen vor grossen Herausforderungen",” Bern, 1 2021. [Online]. Available: <https://www.swissinfo.ch/ger/-die-schweiz-und-ihre-neutralitaet-stehen-vor-grossen-herausforderungen-/46298838>
- [105] DDPS, “Nachbefragung "Sicherheit 2022": Kritischere Betrachtung der Neutralität, grösserer Pessimismus und stärkere Befürwortung der Armee infolge des Krieges in der Ukraine,” Swiss Confederation, Bern, Tech. Rep., 7 2022. [Online]. Available: <https://www.vbs.admin.ch/content/vbs-internet/de/home.detail.nsb.html/89703.html>
- [106] B. Gafner, “Debatte zur Neutralität: Mitmachen bei der Nato ohne Beitritt – geht das überhaupt?” Bern, 8 2022. [Online]. Available: <https://www.derbund.ch/mitmachen-bei-der-nato-ohne-beitritt-geht-das-ueberhaupt-367924030858>
- [107] G. Häsler, “Eine selbstbewusste Neutralität bleibt im Interesse der Schweiz,” Zurich, 8 2022. [Online]. Available: <https://www.nzz.ch/meinung/eine-selbstbewusste-neutralitaet-bleibt-im-interesse-der-schweiz-ld.1699458>
- [108] F. Schäfer, T. Gafafer, and D. Biner, “Cassis wird neutralisiert – seine Bundesratskollegen sind nicht "kooperativ" und weisen den Neutralitätsbericht zurück,” Zurich, 9 2022. [Online]. Available: <https://www.nzz.ch/schweiz/neutralitaetsbericht-cassis-bundesratskollegen-kooperativ-ld.1701616>
- [109] The Federal Council, “Micheline Calmy-Rey,” 6 2017. [Online]. Available: <https://www.admin.ch/gov/en/start/federal-council/members-of-the-federal-council/micheline-calmy-rey.html>
- [110] FDFA, “Die Schweiz im UNO-Sicherheitsrat,” Swiss Confederation, Bern, Tech. Rep., 6 2022. [Online]. Available: <https://www.eda.admin.ch/eda/de/home/aussenpolitik/internationale-organisationen/vereinte-nationen/schweizer-engagement/UNO-Sicherheitsrat.html>
- [111] Federal Chancellery, “Eidgenössische Volksinitiative 'Für eine neutrale weltoffene und humanitäre Schweiz (Neutralitätsinitiative)',” 10 2022. [Online]. Available: <https://www.bk.admin.ch/ch/d/pore/vi/vis416.html>

- [112] M. Kofman, K. Migacheva, B. Nichiporuk, A. Radin, O. Tkacheva, and J. Oberholtzer, “Lessons from Russia’s Operations in Crimea and Eastern Ukraine,” RAND Corporation, Santa Monica (CA), Tech. Rep., 2017. [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1498/RAND_RR1498.pdf
- [113] H. Bolliger, “Neutralität mit Spielraum,” Bern, 3 2003. [Online]. Available: <https://www.swissinfo.ch/ger/neutralitaet-mit-spielraum/3224738>
- [114] P. Murphy, “February 23, 2022 Ukraine-Russia news | CNN,” Atlanta (GA), 2 2022. [Online]. Available: https://edition.cnn.com/europe/live-news/ukraine-russia-news-02-23-22#h_d115a65e9b6348752422ad427fa83b95
- [115] OSCE, “OSCE | Organization for Security and Co-operation in Europe.” [Online]. Available: <https://www.osce.org/whatistheosce>
- [116] Keystone-SDA, “Switzerland elected to UN Security Council,” Bern, 6 2022. [Online]. Available: <https://www.swissinfo.ch/eng/switzerland-elected-to-un-security-council/47661050>
- [117] FDFA, “Switzerland’s election to the UN Security Council,” Swiss Confederation, Bern, Tech. Rep., 6 2022. [Online]. Available: <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-89193.html>
- [118] Federal Administration, “Spiez Laboratory.” [Online]. Available: <https://www.spiezlab.admin.ch/en/home.html>
- [119] Oxford English Dictionary, “neutrality, n. : Oxford English Dictionary,” p. online, 2022. [Online]. Available: <http://www.oed.com/view/Entry/126461?redirectedFrom=neutrality#eid>
- [120] L. Mäder, “Wenn der feindliche Zugang zum Computer gleich mitgeliefert wird,” Zurich, 3 2019. [Online]. Available: https://www.nzz.ch/schweiz/wenn-der-feindliche-zugang-zum-computer-gleich-mitgeliefert-wird-ld.1467220?mktcid=nled&mktcval=107&kid=_2019-3-18
- [121] SZ.de, “Massive Cyberattacke gegen Internationales Rotes Kreuz,” Munich, 1 2022. [Online]. Available: <https://www.sueddeutsche.de/politik/hacker-rotes-kreuz-cyberangriff-1.5511278>

- [122] L. Mäder, “Cyberangriff auf das IKRK: Dahinter steckt wohl ein Staat,” Zurich, 2 2022. [Online]. Available: <https://www.nzz.ch/technologie/hinter-dem-cyberangriff-auf-das-internationale-rote-kreuz-duerfte-ein-staat-stehen-ld.1670318>
- [123] FDFA, “Eleven norms of responsible state behaviour in cyberspace,” 4 2021. [Online]. Available: <https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html>
- [124] Directorate of International Law, “Switzerland’s position paper on the application of international law in cyberspace - Annex UN GGE 2019/2021,” FDFA, Tech. Rep., 2021. [Online]. Available: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf
- [125] Federal Assembly of the Swiss Confederation, “Bundesgesetz über die Armee und die Militärverwaltung,” pp. 1–60, 1995.
- [126] Swiss Department of Defence Civil Protection and Sport, “Das neue Nachrichtendienstgesetz der Schweiz,” 2020. [Online]. Available: <https://www.vbs.admin.ch/de/themen/nachrichtenbeschaffung/nachrichtendienstgesetz.html>
- [127] Swiss Federal Council, “Cyber-Spionage-Angriff auf RUAG,” Federal Department of Defence, Civil Protection and Sport, Bern, Tech. Rep., 5 2016. [Online]. Available: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-61618.html>
- [128] GovCERT.ch, “Technical Report about the Malware used in the Cyberespionage against RUAG,” 5 2016. [Online]. Available: <https://www.govcert.ch/whitepapers/apt-case-ruag-technical-report-govcert-ch/>
- [129] T. Knellwolf, “Cyberangriffe aus Moskau,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/schweiz/standard/cyberangriffe-aus-moskau/story/10479446>
- [130] NZZ.ch, “Geschäftsprüfungsdelegation wollte Geheimhaltung aufheben,” Zürich, 5 2016. [Online]. Available: <https://www.nzz.ch/schweiz/aktuelle-themen/industriespionage-ruag-und-vbs-von-hackern-angegriffen-ld.17914>

- [131] T. Knellwolf, “Cyber-Attacke auf die Ruag: Bundesrat setzt Taskforce ein,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/schweiz/standard/cyberattacke-auf-die-ruag-bundesrat-setzt-taskforce-ein/story/29638139>
- [132] G. Knupfer and K. Merkel-Gyger, “Ruag-Hackerangriff: "Es war Russland",” Zurich, 5 2016. [Online]. Available: <https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536>
- [133] NZZ, “Rüstungsfirma des Bundes gehackt,” Zurich, p. 15, 5 2016.
- [134] Secretariat of the Control Delegation, “Cyber-Angriff auf die RUAG: begleitende Oberaufsicht durch die GPDel,” The Swiss Parliament, Bern, Tech. Rep., 5 2016. [Online]. Available: <https://www.parlament.ch/press-releases/Pages/mm-gpdel-2016-05-04.aspx>
- [135] T. Knellwolf, “Russische Hacker mit totalem Zugriff,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/russische-hacker-mit-totalem-zugriff-938519431408>
- [136] A. Fossgreen, “Geheime Schweizer Elitetruppe enttarnt,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/geheime-schweizer-elitetruppe-enttarnt-785088675289>
- [137] S. Bühler and A. Schmid, “Russische Hacker enttarnen geheime Schweizer Elitetruppe,” Zurich, 5 2016. [Online]. Available: <https://www.nzz.ch/nzzas/cyber-attacke-gegen-ruestungskonzern-ruag-russische-hacker-enttarnen-geheime-schweizer-el-18562>
- [138] I. Städler and T. Knellwolf, “Fall Ruag: Bund fürchtet das Schlimmste,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/fall-ruag-bund-fuerchtet-das-schlimmste-397155128050>
- [139] T. Knellwolf, “Ruag-Spionage: Outlook-Daten betroffen,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/ruag-spionage-outlook-daten-betroffen-773858623632>
- [140] derbund.ch, “Bund war wohl das Ziel der Ruag-Hacker,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/bund-war-wohl-das-ziel-der-ruag-hacker-184482839845>

- [141] L. Häuptli, “Hackerabwehr: Dem Geheimdienst sind die Hände gebunden,” Zurich, pp. 1,10,11, 5 2016.
- [142] ———, “Firmen müssen sich selbst vor Hackerangriffen schützen,” Zurich, p. 10, 5 2016.
- [143] S. Bühler and A. Schmid, “Ruag: Cyberattacke zielte auf VBS,” Zurich, p. 11, 5 2016.
- [144] swissinfo.ch, “Defence firm says no sensitive data acquired in hack,” Bern, 5 2016. [Online]. Available: https://www.swissinfo.ch/eng/ruag-breach_defence-firm-says-no-sensitive-data-acquired-in-hack/42151696
- [145] derbund.ch and SDA, “Ruag-Hacker haben 20 Gigabyte Daten entwendet,” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/ruag-hacker-haben-20-gigabyte-daten-entwendet-377578029665>
- [146] N. Jürgensen, “Mehr als 20 Gigabyte Daten entwendet,” Zurich, 5 2016. [Online]. Available: <https://www.nzz.ch/cyber-spionage-angriff-auf-ruag-mehr-als-20-gigabyte-daten-entwendet-ld.84138>
- [147] Swiss Federal Council, “Erkenntnisse im Zusammenhang mit Cyber-Spionage-Angriff auf RUAG,” Federal Department of Defence, Civil Protection and Sport, Bern, Tech. Rep., 5 2016. [Online]. Available: <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-61788.html>
- [148] M. Surber, “Cyberangriff auf Ruag – Lob und Tadel für das Verteidigungsdepartement | NZZ,” Zurich, 5 2018. [Online]. Available: <https://www.nzz.ch/schweiz/cyberangriff-auf-ruag-lob-und-tadel-fuer-das-verteidigungsdepartement-ld.1384399>
- [149] Secretariate of the Control Committees, “Cyberangriff auf die RUAG: Angemessene Massnahmen des Bundesrates und des VBS, aber ungenügende strategische Steuerung,” The Swiss Parliament, Bern, Tech. Rep., 5 2018. [Online]. Available: <https://www.parlament.ch/press-releases/Pages/mm-gpk-n-2018-05-08.aspx>

- [150] M. Häfliger, “Die Ruag enthält dem Bund Informationen vor,” Bern, 5 2018. [Online]. Available: <https://www.derbund.ch/die-ruag-enthaelt-dem-bund-informationen-vor-196310670805>
- [151] NZZ.ch, “Bundesanwaltschaft sistiert Verfahren zu Cyberangriff auf Ruag,” Zurich, 8 2018. [Online]. Available: <https://www.nzz.ch/schweiz/bundesanwaltschaft-sistiert-verfahren-zu-cyberangriff-auf-ruag-ld.1414744>
- [152] A. Hardegger and L. Mäder, “Ruag: Der Rüstungskonzern soll grösstenteils privatisiert werden,” Zurich, 3 2019. [Online]. Available: <https://www.nzz.ch/schweiz/ruag-der-ruestungskonzern-soll-groesstenteils-privatisiert-werden-ld.1467996>
- [153] C. P. Federal Department of Defence and Sport, “Sicherheit Schweiz 2016,” Federal Intelligence Service, Bern, Tech. Rep., 2016. [Online]. Available: <https://www.vbs.admin.ch/de/vbs/organisation/verwaltungseinheiten/nachrichtendienst.detail.document.html/vbs-internet/de/documents/nachrichtendienst/lageberichte/NDB-Lagebericht-2016-d.pdf.html>
- [154] T. Knellwolf, “"Als ich am WEF war, wurde mein Departement attackiert",” Bern, 5 2016. [Online]. Available: <https://www.derbund.ch/als-ich-am-wef-war-wurde-mein-departement-attackiert-551370787903>
- [155] F. Brunton, *Spam: A Shadow History of the Internet*, ser. Infrastructures series. Cambridge, MA: MIT Press, 2013.
- [156] The Swiss Parliament, “Control Delegation.” [Online]. Available: <https://tinyurl.com/yhmmzt3p>
- [157] Persoenlich.com, “Medienqualitätsrating: Das sind die besten Schweizer Medien - Medien,” 9 2016. [Online]. Available: <https://www.persoenlich.com/medien/das-sind-die-besten-schweizer-medien>
- [158] SonntagsZeitung, “Personaldaten des Bundes in Putins Händen,” Zurich, 5 2016. [Online]. Available: http://sonntagszeitung.ch/read/sz_08_05_2016/nachrichten/Personaldaten-des-Bundes-in-Putins-Haenden-63403
- [159] J. Wurz, “Paper claims special forces unit exposed by hack,” Bern, 5 2016. [Online]. Available: https://www.swissinfo.ch/eng/ruag-affair_sensitive-personal-information-likely-hacked/42140796

- [160] RUAG, “Cyber attack on RUAG: major damage averted,” RUAG, Bern, Tech. Rep., 5 2016. [Online]. Available: <https://www.ruag.com/en/news/cyber-attack-ruag-major-damage-averted>
- [161] National Council, “Aufklärung des Cyberangriffs auf die Ruag,” Bern, 6 2016. [Online]. Available: <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161022>
- [162] —, “Cyberattacke auf die Ruag und das VBS. Die notwendigen Konsequenzen ziehen!” 6 2016. [Online]. Available: <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161021>
- [163] Parliamentary Control Committee, “Standortbestimmung: Bewältigung des Cyber-Angriffs auf die RUAG,” The Swiss Parliament, Bern, Tech. Rep., 5 2018.
- [164] M. Stolz, “Platform Neutrality – A Solution for the Social Media War?” in *16th International Conference on Cyber Warfare and Security*. Online: ACI, UK, 2021, pp. 336–344.
- [165] M. S. Stolz, “Platform Neutrality and the Global Balance of Powers,” in *CSCI-ISNA: Social Network Analysis, Social Media, & Mining*. IEEE CPS, 2021.
- [166] Conseil National du Numérique, “Platform Neutrality (57),” Ministère de l’économie du redressement productif et du numérique, Paris, Tech. Rep. May, 2014.
- [167] W. Gao and Y. Yang, “Chaining cyber-titans to neutrality: An updated common carrier approach to regulate Platform Service Providers,” *Computer Law and Security Review*, vol. 31, no. 3, pp. 412–421, 2015. [Online]. Available: <http://dx.doi.org/10.1016/j.clsr.2015.03.003>
- [168] Jan Krämer and D. Schnurr, “Is there a need for platform neutrality regulation in the EU?” *Telecommunications Policy*, vol. 42, no. 7, pp. 514–529, 2018. [Online]. Available: <https://doi.org/10.1016/j.telpol.2018.06.004>
- [169] W. H. Dutton, “The Fifth Estate: Canaries in the Institutions of Liberal Democracies,” in *Politische Komplexität, Governance von Innovationen und Policy-Netzwerke. Festschrift für Volker Schneider*, M. Nagel, P. Kenis, P. Leifeld, and H.-J. Schmedes, Eds. Wiesbaden: Springer VS, 2020, ch. 7, pp. 59–65.

- [170] J. Schmitz, E. M. Rogers, K. Phillips, and D. Paschal, "The public electronic network (PEN) and the homeless in Santa Monica," *Journal of Applied Communication Research*, vol. 23, no. 1, pp. 26–43, 2 1995. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/00909889509365412>
- [171] AVAAZ, "Facebook's Algorithm: A Major Threat to Public Health," 8 2020.
- [172] R. Stauffacher, "Studie von Avaaz zu Covid-19: Facebook versinkt in den Fake-News," Zurich, 2020. [Online]. Available: https://www.nzz.ch/technologie/studie-von-avaaz-zu-covid-19-facebook-versinkt-in-den-fake-news-ld.1572117?mktcid=nled&mktcval=165_2020-08-20&kid=_2020-8-19&ga=1&trco=
- [173] —, "Wie sich Facebook und Co. in der Corona-Krise als Helfer in der Not profilieren," Zurich, 2020. [Online]. Available: <https://www.nzz.ch/technologie/coronavirus-facebook-profiliert-sich-als-helfer-in-der-not-ld.1547415>
- [174] T. Hatmaker, "Facebook will put a new coronavirus info center on top of the News Feed | TechCrunch," 3 2020. [Online]. Available: https://techcrunch.com/2020/03/18/facebook-coronavirus-information-center-zuckerberg/?guccounter=1&guce_referrer=aHR0cHM6Ly9nZXRwb2NrZXQuY29tLw&guce_referrer_sig=AQAAAAvYgmWRmC6_bHrV5gAI5o3-4269v5bnkLjJ4kK1cTaG43s7HvYiHd8_u_BtGqCfbQ6r1eiDXMKFNE4y9R-8GsXqX
- [175] J. Thier, "Coronavirus bringt Facebook in die Bredouille," Zurich, 3 2020. [Online]. Available: https://www.nzz.ch/meinung/das-coronavirus-bringt-facebook-in-bredouille-ld.1549415?mktcid=nled&mktcval=165_2020-04-01&kid=_2020-3-31&trco=
- [176] J. Kormann, "Facebook löscht erstmals Trump-Video zum Coronavirus," Zurich, 8 2020. [Online]. Available: <https://www.nzz.ch/technologie/facebook-loescht-erstmal-trump-video-zum-coronavirus-ld.1570034>
- [177] S. Hurtz, "Facebook und Reddit: Keine Bühne für Rassisten," Munich, 7 2020. [Online]. Available: https://www.sueddeutsche.de/digital/facebook-reddit-rassismus-meinungsfreiheit-1.4970415?sc_src=email_1693663&sc_lid=143972035&sc_uid=HaUGuZAqBR&sc_llid=44302&utm_medium=email&utm_source=emarsys&utm_content=www.sueddeutsche.de%2Fdigital%2Ffacebook-reddit-

- [178] —, “Werbeboykott: Facebook steht unter Druck wie selten zuvor,” Munich, 6 2020. [Online]. Available: https://www.sueddeutsche.de/digital/facebook-werbeboykott-zuckerberg-trump-1.4952718?sc_src=email_1658084&sc_lid=142240009&sc_uid=HaUGuZAqBR&sc_llid=8171&utm_medium=email&utm_source=emarsys&utm_content=www.sueddeutsche.de%2Fdigital%2Ffacebook-werbeboykott
- [179] M.-A. Langer, “Trump rächt sich mit einem Dekret an Twitter und anderen sozialen Netzwerken,” Zurich, 5 2020. [Online]. Available: https://www.nzz.ch/international/trump-unterzeichnet-verfuegung-zur-reglementierung-von-twitter-und-co-ld.1558778?mktcid=nled&mktcval=165_2020-05-29&kid=_2020-5-28&trco=
- [180] NZZ.ch, “Twitter versieht staatsnahe Nutzerkonten mit Symbolen,” Zurich, 8 2020. [Online]. Available: https://www.nzz.ch/panorama/twitter-versieht-staatsnahe-nutzerkonten-mit-symbolen-ld.1570160?mktcid=nled&mktcval=165_2020-08-07&kid=_2020-8-6&ga=1&trco=
- [181] SZ.de, “Twitter kennzeichnet ab sofort staatsnahe Medien,” Munich, 8 2020. [Online]. Available: https://www.sueddeutsche.de/digital/twitter-staatsmedien-warnhinweis-1.4992236?sc_src=email_1736397&sc_lid=146357221&sc_uid=HaUGuZAqBR&sc_llid=54723&utm_medium=email&utm_source=emarsys&utm_content=www.sueddeutsche.de%2Fdigital%2Ftwitter-staatsmedien-warnh
- [182] M. Muth, “Wie Facebook unlautere Wahlwerbung verhindern will,” Munich, 3 2020. [Online]. Available: https://www.sueddeutsche.de/digital/political-ads-werbung-facbeook-europawahl-1.4387893?sc_src=email_624406&sc_lid=69103931&sc_uid=HaUGuZAqBR&sc_llid=57940&utm_medium=email&utm_source=emarsys&utm_content=www.sueddeutsche.de%2Fdigital%2Fpolitical-ads-werbu
- [183] Facebook, “New Steps to Protect the US Elections - About Facebook,” 9 2020. [Online]. Available: <https://about.fb.com/news/2020/09/additional-steps-to-protect-the-us-elections/>
- [184] L. Kamps, “Facebook bereitet sich auf eine Zeit ohne Gewinner vor,” Berlin, 10 2020. [Online]. Available: <https://netzpolitik.org/2020/us-praesidentschaftswahl-facebook-bereitet-sich-auf-eine-zeit-ohne-gewinner-vor/>

- [185] T. Denkler, “Trump sagt Twitter den Kampf an,” Munich, 5 2020. [Online]. Available: https://www.sueddeutsche.de/politik/trump-twitter-usa-1.4920615?utm_source=emarsys&sc_lid=137422731&utm_content=sz.de/1.4920615&utm_campaign=EspressoamMorgen28.5.2020&sc_lid=96001&utm_medium=email&sc_src=email_1571828&sc_uid=HaUGuZAqBR
- [186] M. Isaac and K. Browning, “Zuckerberg and Dorsey Face Harsh Questioning From Lawmakers - The New York Times,” New York City, 11 2020. [Online]. Available: <https://www.nytimes.com/live/2020/11/17/technology/twitter-facebook-hearings>
- [187] NZZ.ch, “Soziale Netzwerke und US-Wahlen: Die Chefs von Facebook und Twitter stellen sich den Fragen der Senatoren ,” Zurich, 11 2020. [Online]. Available: https://www.nzz.ch/technologie/us-wahlen-das-sind-die-herausforderungen-fuer-facebook-und-co-ld.1557220?mktcid=nled&mktcval=108_2020-08-18&kid=nl108_2020-8-21&ga=1
- [188] J. Clayton, “Kamala Harris: Facebook removes racist posts about US vice-president-elect,” London, 11 2020. [Online]. Available: <https://www.bbc.com/news/technology-54941571>
- [189] S. Levy, “The Plain View: Facebook’s Oversight Board,” 2 2020. [Online]. Available: <https://link.wired.com/view/5d727748a777390d4a148d90cwggx.4cfh/deedc305>
- [190] K. Meta Beisel and M. Kolb, “EU will härter gegen Desinformationen vorgehen,” Munich, 6 2020. [Online]. Available: https://www.sueddeutsche.de/politik/eu-kommission-corona-desinformation-bericht-1.4932844?sc_src=email_1602973&sc_lid=139161974&sc_uid=HaUGuZAqBR&sc_lid=91469&utm_medium=email&utm_source=emarsys&utm_content=www.sueddeutsche.de%2Fpolitik%2Feu-kommission-c
- [191] sz.de, “Reaktion auf die Youtube-Sperre von RT DE - Medien - SZ.de,” 9 2021. [Online]. Available: https://www.sueddeutsche.de/medien/youtube-rt-gegenmassnahmen-1.5424905?utm_source=pocket_mylist