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 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 wear 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.

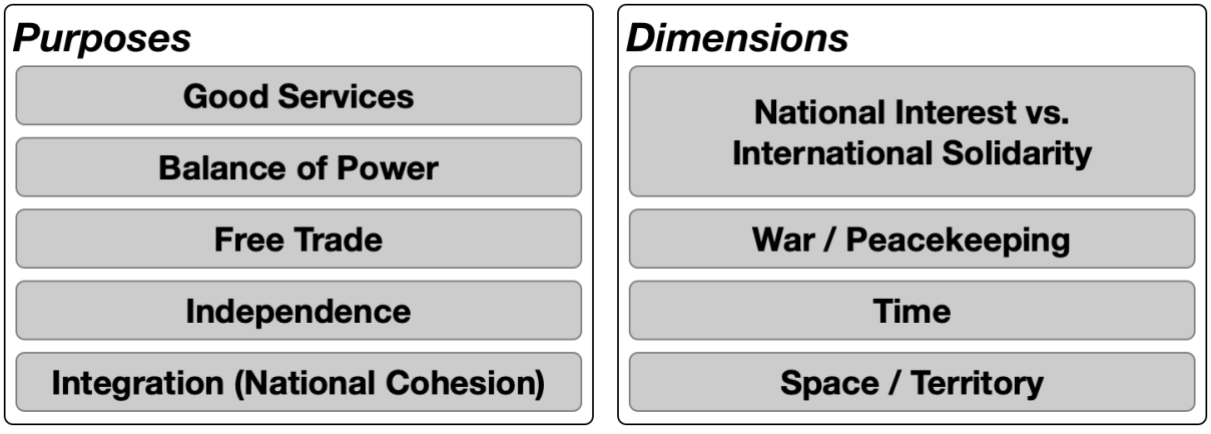

Figure 1: The functions and dimensions of state neutrality, according to Riklin (1991)

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 Budesrat (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%20DFAE%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