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

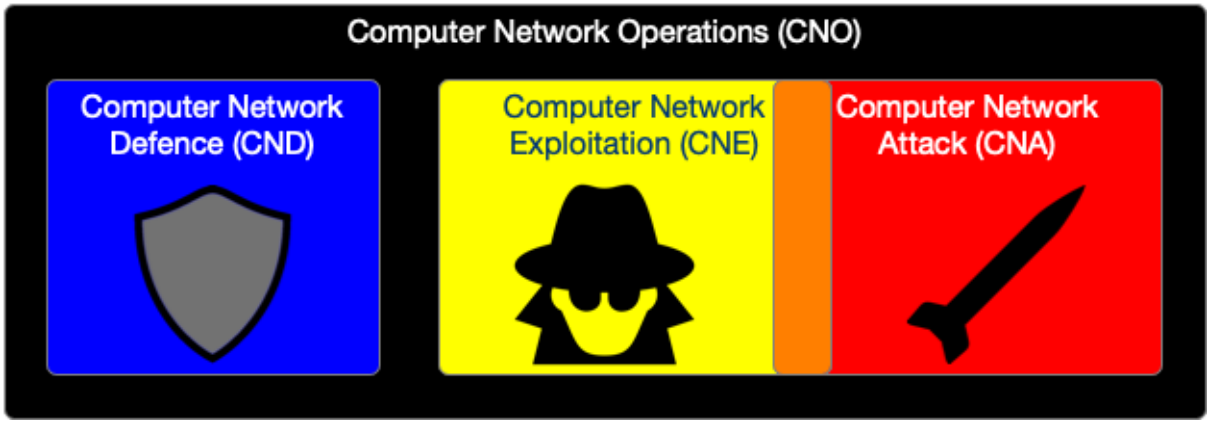
1. Introduction

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 thi 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

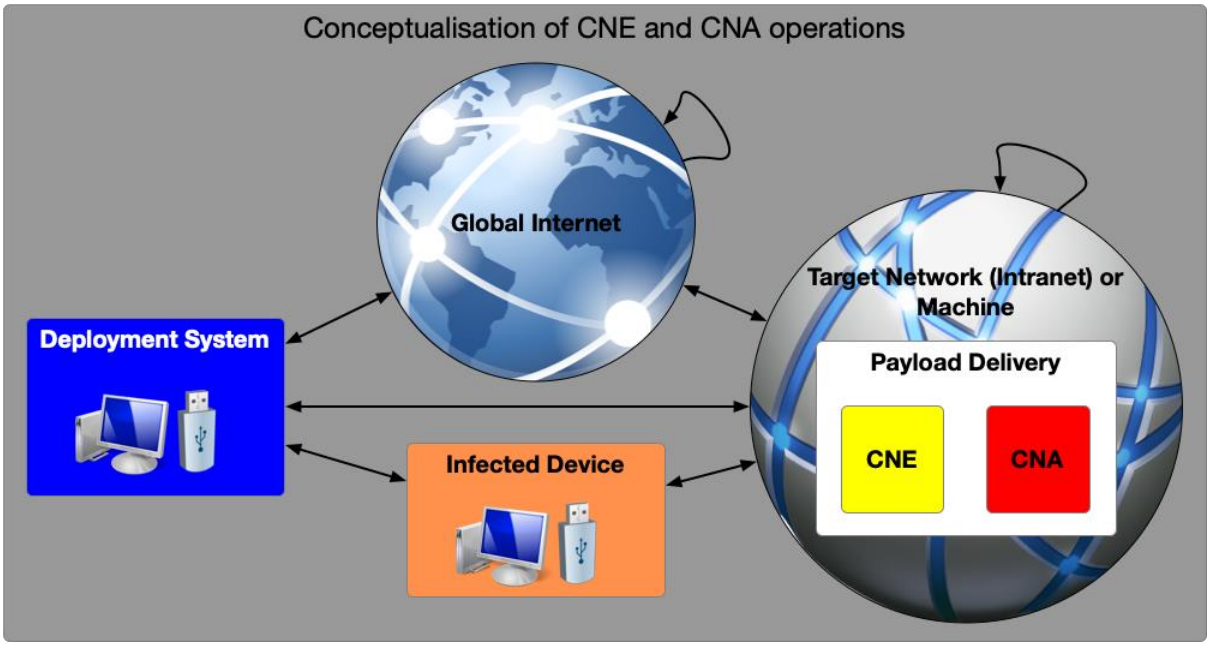
Operations in cyberspace usually involve the exploitation of security holes of computer systems and networks in order to achieve their goal. A technical, high-level conceptualisation of these operations in cyberspace is provided below.

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 involves 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 Confedaration, 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 adminstrativce 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 Ordinnance* 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 incorportaed 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.

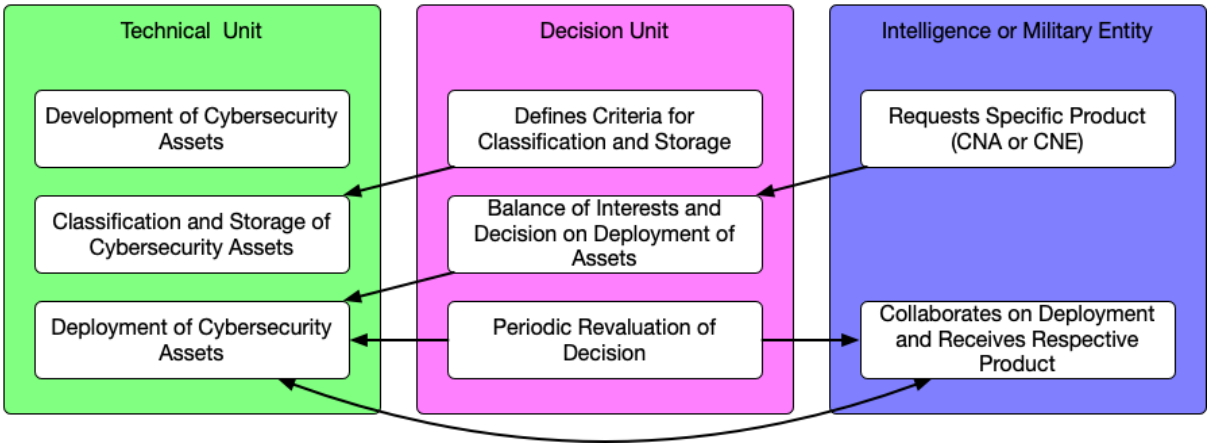
Figure 3 further depicts the role of an intelligence or military / defence entity on the right-hand side. It is suggested that in case a security entity would like to deploy an intrusive cybersecurity operation, i.e., a CNE or CNA operation, it should provide a detailed technical request to the Decision 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 Innnern (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.