ICT for peace foundation

POLICY BRIEF

SWISS NEUTRALITY IN THE AGE OF CYBER WARFARE

Martin Dahinden

GENEVA 2021

ICT4Peace Foundation

ICT4Peace Publishing, Geneva. January 2021
Copies available from www.ict4peace.org

SWISS NEUTRALITY IN THE AGE OF CYBER WARFARE

Martin Dahinden

ICT for peace foundation

Discussion paper

SWISS NEUTRALITY IN THE AGE OF CYBER WARFARE

Martin Dahinden[1]

Cyber warfare is a new and significant challenge for Swiss neutrality. Based on the law of neutrality and Swiss neutrality policy, this discussion paper outlines important legal, political and conceptual issues. First and foremost, it is a contribution to an emerging debate, but it points also to opportunities that arise for Switzerland in the changing environment.[2]

INTRODUCTION

The questions about the rights and obligations of neutral states in cyberspace are complex and can by no means be answered with simple deductions from neutrality law and conventional neutrality policy.

Today, there is a broad international consensus that international law is also applicable to cyberspace. However, legal opinions and political attitudes differ widely as to what this means in concrete terms for the individual norms of international law. This conclusion must be drawn in particular from the deliberations that have taken

1 Martin Dahinden was Swiss Ambassador to the USA, is a member of the Foundation Board of the Think Tank ICT4Peace and teaches security policy at the University of Zurich.

2 I would like to thank Sanija Ameti, Anne-Marie Buzatu, Serge Droz, Alain Modoux, Sara Pangrazzi, Daniel Stauffacher and Regina Surber for their comments and inputs.

place over the past few years within the framework of the UN.[3] The understanding of the problem has been deepened; in part, common views have been formulated. However, a real breakthrough in the critical questions and binding norms has not yet been achieved, because political differences cannot be solved by formulating legal opinions.

The law of neutrality has been an issue, directly or indirectly, in the international forums dealing with cyber issues. It is obvious that in the age of cyber warfare there will be conflicts and third states that do not participate in them as well. For these third states, the rights and obligations of a neutral state apply. It is therefore not surprising that the Tallinn Manual[4] contains a special chapter on neutrality.

However, Switzerland's permanent neutrality goes far beyond the core of neutrality law. Even in times of peace, Switzerland follows a policy that makes credible that the country will remain neutral in future international armed conflicts.

Cyber space is new domain with many special features. For this reason, Switzerland's neutrality policy for the age of cyber warfare cannot simply be derived from existing

3 See United Nations Group of Governmental Experts on Information Security (UNGGE). The UNGGE was created in 2004 by the First Committee of the UN General Assembly with the aim of advising on how peace and security in cyberspace can be strengthened through confidence-building measures and norms for responsible state behavior, as well as building the necessary capacities. See also the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG) established in parallel by the United Nations in 2018. Fact sheet Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019-2021: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf.
ICT4Peace has been supporting the UN GGE and UN OEWG processes since 2011 through expert reports, concrete proposals and training programs for diplomats and senior officials. The aim is to promote responsible behavior by states, confidence-building measures, norms and the development of the necessary state capacities (Cf. overview: https://ict4peace.org/?category_name=support-to-un-oewg-and-un-gge&s=&load=all

4 Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (2017). Cambridge: Cambridge University Press. The Tallinn Manual is an academic study on the applicability of the international law of war to cyber conflicts and cyber wars (ius ad bellum; ius in bello). The Tallinn Manual was written by around twenty experts between 2009 and 2012 at the invitation of the NATO Cooperative Cyber Defence Center of Excellence.

doctrines on neutrality policy but requires above all fresh security policy thinking.[5]

Permanent neutrality is the basis for Switzerland's special role in the community of states. Because advantages arise from permanent neutrality, Switzerland has always understood its neutrality status as a duty to make a special contribution to peace and security in the world. This includes, among other things, humanitarian engagement, the willingness to render good offices, efforts to strengthen international law, commitment to confidence-building measures, conflict prevention and conflict management. How can and should this role be fulfilled in the age of cyber warfare?

1. NEUTRALITY AS A PRINCIPLE OF SWISS FOREIGN POLICY

Permanent neutrality is a central principle of the Swiss self-conception and of Swiss foreign policy. It is, however, not a constitutional objective in itself but serves to safeguard the independence of the country and the inviolability of its territory. For this reason, neutrality is not mentioned either in the article of purpose or in the foreign policy principles of the Federal Constitution.[6]

The law of neutrality was codified in the Hague Conventions of 18 October 1907[7] and is now part of customary international law. It defines the rights and obligations of a neutral state.

5 See Dahinden, Martin, Pangrazzi, Sara (2020): Neutralität im Cyberraum: Die Schweiz ist gefordert. Neue Zürcher Zeitung, (NZZ) 31.12.2020, 19

6 This section is follows the official presentation of neutrality by the Federal Department of Foreign Affairs (FDFA).

7 https://www.admin.ch/opc/de/classified-compilation/19070029/index.html

The most important of these rights is the inviolability of the state's territory. The most important obligations of the neutral state are,

- not to take part in international armed conflict;
- to ensure its own self-defense;
- to treat all belligerents equally with regard to the export of arms;
- not to provide troops or mercenaries to the belligerents;
- not to place its own territory at the disposal of the belligerents.

The right of neutrality applies to conflicts between states. It does not apply to military operations authorized by the United Nations Security Council. Like all states, neutral states have the right to self-defense in the event of an armed attack.

The neutrality policy consists of the totality of measures taken by a neutral state to make its neutrality status credible. The concrete form of neutrality policy depends strongly on the international environment and its assessment. Accordingly, neutrality policy is subject to considerable change over time which leads to an actual practice that ultimately extends far beyond the legal core of neutrality.

2. THE CHALLENGE OF CYBERSPACE

Information and communication technologies (ICT) hold unprecedented potential for social and economic development, but at the same time pose great risks to peace and international security.

In the meantime, many states have built up ICT capacities for military purposes and continue to expand them on a large scale. This has created a new, fourth dimension of warfare in addition to land, sea and air warfare.

Three main types of cyber operations can be distinguished in this context:

1. **Computer network exploitations** (CNE) are operations that penetrate foreign networks in order to steal information, ideally without leaving any traces.
2. **Computer Network Attacks** (CNA) are attacks on systems to disrupt, damage

or even destroy them, including the stored information. CNAs are the greatest risks, especially when they are directed against critical infrastructure.

3. **Information Operations** (IO) influence opinions in a foreign state in favor of one's own intentions.[8]

Typically, cyber-attacks are part of hybrid warfare, i.e., they occur in combination with regular and irregular, symmetric and asymmetric, military and non-military, overt and covert forms of combat.[9] In cyber operations, it is often difficult to identify the originators of attacks (attribution). It is also difficult to determine which activities and at what level of intensity constitute an attack or an armed conflict. Often it is even difficult to determine whether an attack has occurred at all or whether it is collateral damage.[10]

In traditional neutrality law, the state territory plays an important role for the rights and obligations of the neutral state. State territory is also relevant in the age of cyber warfare, as national legal systems and de facto control continue to have a geographical dimension. However, the physically elusive cyberspace leads to a complexity that exceeds previous experience.

It makes sense to understand the cyberspace, the Internet, as a global public good, without thereby neglecting the sovereignty of states with regard to facilities, persons, intellectual property, etc. Such a view is not widespread, probably because it links a political-economic concept (global commons) with legal categories.

Cyberspace and cyber warfare are particularly complex because not only states but almost anyone can become a player and because the fundamental distinction in international humanitarian law between civilians and combatants is particularly unclear.

---

8 See Meyer, Paul, Stauffacher, Daniel (2021): Neue Zürcher Zeitung (NZZ), 11 February 2021

9 See Countering Hybrid Warfare Project (CHW): https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare. Hoffman, Frank G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies.

10 ICT operations are also used for terrorist purposes or by criminal organizations. However, they are not the subject of this discussion paper, which focuses on the neutrality aspects. See https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2016-Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf

3. NEUTRALITY IN CYBERSPACE

The following sections deal with neutrality in cyberspace in legal and political terms. They provide an overview, raise questions and - as far as possible – sketch answers. The argumentation follows the order of the most important rights and obligations for neutrals, as mentioned above.

Inviolability of national territory

The most important right of a neutral state is the inviolability of its national territory. But what does the inviolability of state territory mean in the context of cyber operations and cyber warfare? Is it about physical effects (damage to people and objects)? Is it also about infrastructure and the functioning of internet-based instruments? Is it about comprehensive protection of digital space under the control and legal jurisdiction of a state?

The inviolability of their national territory is, of course, a right of all states, not just neutral ones. The international discussions in this area are of direct importance for Switzerland.

Self-defense in the event of cyber attacks

According to Article 51 of the UN Charter, states that are attacked have the legitimate right to self-defense. This is an exception to the general prohibition of the use of force in the UN Charter.

However, the question of the threshold at which an attack reaches a level that legitimizes the attacked state to take action against an aggressor with digital or even kinetic means is disputed.[11] Here, too, it is not only a matter of legal classification, but ultimately of political decisions as to when and by what means the right to self-defense is invoked. Corresponding doctrines can have a dissuasive effect or lead to escalation.

11 Pangrazzi, Sara (2021): Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, ICT4Peace Publishing, Geneva. January 2021

This problem concerns all states. However, it is of particular importance for the neutral state because it is also about whether a cyber-attack "only" violates neutrality or at what intensity the neutral state itself becomes a party to an armed conflict.

Cooperation in the areas of protection and defense

Cooperation with other states in the areas of protection is compatible with the status of neutrality, but it is a delicate area because dependencies can arise, and the credibility of neutrality can be impaired in the event of a conflict. While joining a defense alliance is not compatible with neutrality, exchange of experience, training and armament cooperation, etc. perfectly are.

What is the situation in the cyber area? What concrete forms of cooperation are possible without creating uncertainty as to whether the neutral state can and will actually be neutral in the event of a conflict? Are there legal limits (agreements, etc.) or limits of a factual nature (shared infrastructure, interoperability, etc.)?

The UN recommends[12] that states be supported if their infrastructure is exposed to a cyber-attack. Under what conditions is support by a neutral state unobjectionable (similar to humanitarian aid)? When does it become support for a party to a conflict that is inadmissible under neutrality law?

Non-participation in armed conflicts

The neutral state is prohibited from participating in armed conflicts. Of course, this is also the case if a conflict is fought in whole or in part by digital means.

At first glance, this provision seems very unambiguous. However, it presupposes that it is clear whether an armed conflict exists at all. The topic leads back to the questions of the threshold of war, the classification of cyber-attacks and the problem of hybrid warfare.

12 UN General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, UN Doc. A/70/174 (UN GGE Report 2015)

Ensuring self-defense

The provision that neutral states must ensure their own self-defense serves the credibility and predictability of neutrality.

What does such an obligation mean in the age of cyber warfare? By analogy with conventional warfare, it means that the neutral state is obliged to protect its infrastructure in such a way that it cannot be used by parties to the conflict. A neutral state that does not protect itself or fails to take reasonable protective measures would therefore not be fulfilling the obligations of a neutral state. Irrespective of the issue of neutrality, the UN also demands that states implement protective measures against cyber-attacks.[13]

But what concrete precautions are necessary? What is reasonable? Is it about passive protective measures (firewalls, denial of access to infrastructure, protection against malware, etc.)?[14] What about threats that do not take place on the own territory, for example a phishing site that is used to collect access data? Is a deterrent offensive cyber capacity necessary and permissible to prevent cyber operations?

This leads to the delicate question of the extent to which the neutral state itself should have offensive cyber capacities at its disposal in order to be able to act preventively and pre-emptively. In terms of neutrality policy, restraint might be called for. However, there are at least two arguments in favor of an offensive cyber capacity. Firstly, it is difficult to imagine that effective protective measures against cyber-attacks can be built up without having the corresponding capabilities at one's disposal. Secondly, the neutral state cannot rule out the possibility that it may itself be attacked and wish to exercise the right to self-defense under Article 51 of the UN Charter.

Equal treatment of all warring parties with regard to the export of armaments

When exporting armaments (equipment, technology), the neutral party must treat all warring parties equally. This is not a ban, but a prohibition of discrimination.

13 UN GGE Report 2015

14 Cf. Basic cyber security measures of the German Federal Office for Information Security: https://docplayer.org/114578396-Basismassnahmen-der-cyber-sicherheit.html

Switzerland's war material export policy is by far not only about checking compatibility with the law of neutrality and neutrality policy, but also about far-reaching foreign policy objectives (human rights, development policy, etc.).[15] How should against this background export of goods and technologies intended for cyber warfare be handled.

Devices and technologies used for cyber warfare are largely dual-use goods, i.e., goods that can be used for both civilian and military purposes. In this respect, they have similar characteristics to dual-use goods in missile technology or in the nuclear, biological and chemical sectors, where international export control regimes exist. Switzerland is by principle in favor of multilateral control measures against the undesired proliferation of dual-use goods.

Such a control regime does not exist for the cyber domain. Certain devices and technologies are controlled under the Wassenaar Arrangement. There is little prospect of effective multilateral export controls emerging in this or any other framework in the foreseeable future. It is likely that the USA, China and the EU will introduce unilateral controls and put pressure on third countries such as Switzerland, which can be sensitive in terms of neutrality policy and, in the event of conflict, also in terms of neutrality law.[16]

Sanctions

The UN Security Council has the power to impose sanctions that are legally binding on all states. States can also impose sanctions alone or jointly with others in order to pursue foreign policy goals, such as compliance with international law or respect for human rights. Such sanctions are only rarely directly related to the law of neutrality. However, like export controls, they can affect the credibility of the neutral state. This also applies to sanctions that would be taken as a measure against cyber operations.

15 Article 5 Swiss War Material Ordinance (https://www.fedlex.admin.ch/eli/cc/1998/808_808_808/de)

16 Cf. Holzer, Patrick Edgar (2020): Das Güterkontrollgesetz (Definitions in the Goods Control Act. In: Cottier, Thomas, Oesch, Matthias (eds.) Schweizerisches Bundesverwaltungsrecht Band XI, Allgemeines Aussenwirtschafts- und Binnenmarktrecht. Basel: Helbing Lichtenhahn Verlag, 147-230. Publications of the Wassenaar Arrangement: https://www.wassenaar.org

Prohibition on providing troops or mercenaries to warring parties

Neutral states may not provide troops or mercenaries to warring parties and may not allow recruitment on their own territory.

How should a neutral state behave towards private companies and individuals who are active on its territory in the field of cyber security and offer technologies or services for cyber operations? The respective provisions of neutrality law go in some cases beyond non-discrimination and require specific prohibitions. The problem is analogous to that of private security companies. It is therefore worthwhile to examine the issue in greater depth by analogy with the Montreux Document and the Montreux Process - not only from the point of view of human security, but also from the point of view of neutrality.[17]

There is also a need for clarification with regard to terms such as soldier and mercenary. What do they mean in the context of cyber warfare? Is it exclusively about people who use digital resources as a means of combat or do bots, bot farms, etc. also fall under this term? And what about state responsibility in this context?

Prohibition of making one's own national territory available to the warring parties

Neutrals are prohibited from making their national territory available to the warring parties. This obligation is a prohibition that goes beyond non-discrimination.

The Hague Convention of 18 October 1907 contains provisions on wireless radio communications. According to these provisions, neutral states may not permit such equipment on their territory if it serves the traffic between the armed forces of belligerent states (Article 3). On the other hand, they are not obliged to prohibit the belligerents from using their territory for other wireless radio communication (Article 7).[18]

17 Cf FDFA, Montreux document: https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-law/international-humanitarian-law/private-military-security-companies/montreux-document.html

18 Agreement concerning the Rights and Duties of Neutral Powers and Persons in the Event of a terrestrial war, Article 3 and Article 7: https://www.fedlex.admin.ch/eli/cc/26/499_376_481/de

By analogy, this would probably mean that the neutral state may not permit the use of its infrastructure (servers, communication networks, etc.) for the cyber warfare of other states. However, even in the case of an armed conflict, it would not be obliged to prevent all (i.e., also civilian) use of ICT capacity. Such a compartmentalization is not simple and requires clarification. Consider, for example, information operations in the context of hybrid warfare, where it is not always possible to identify what ICT infrastructure is used to disseminate information.

It should be noted that the UN experts demand that states do not knowingly allow their territory to be used for acts contrary to international law using ICT.[19]

4. FOOD FOR THOUGHT FOR PEACE AND MORE SECURITY IN CYBERSPACE

Swiss neutrality policy shapes Swiss foreign policy far beyond the core of the law of neutrality and beyond neutrality doctrines. It is anchored in historical experience and Switzerland's political culture. There is no reason to abandon these policies because new forms of conflict and weaponry emerge. But it is necessary and urgent to consider how contributions to peace and security can be made in the age of cyber warfare.

The spectrum of possible action is wide. The following sections are by no means comprehensive but rather indications of paths worth considering.

Good offices

Neutral states are particularly suited to providing good offices. Today, good offices mean all kinds of assistance to third parties (protecting power mandates, hosting international conferences and organizations, fact-finding, contributions to the peaceful settlement of disputes, etc.).

19 "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs … States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-State actors to commit such acts;" (UN GGE Report 2015).

The financial support of fact-finding activities (attribution of cyber incidents to fact-checking in connection with information operations) is a field of activity that fits well in the tradition of good offices. So is the support of initiatives such as FIRST (Forum for Incident Response and Security Teams).[20]

The promotion of Switzerland as a center of governance and efforts to make Geneva a platform for cooperation in the digital field are to be considered as part of this effort creating synergies with already existing multilateral structures.[21]

Confidence-building measures

Confidence-building measures have great potential to prevent and mitigate conflicts. They are often provided within the framework of international agreements or international organizations. A neutral state can provide effective support by using its credibility to put forward proposals and, if necessary, implement confidence-building measures itself.

During the deliberations within the UN, a consensus was reached that stronger cooperation and more transparency are suitable for reducing conflict risks. Voluntary confidence-building measures have also been identified. Although states bear the main responsibility, it is important that the private sector, academia and civil society are also involved in finding solutions.[22] Switzerland can make a special contribution to this with its direct and uncomplicated dealings with different interest groups.[23]

20 The Forum for Incident Response and Security Teams (FIRST) is an international association of individual CERTs that work together to exchange technical and security-related information. It has over 220 members from 42 countries. Member incident response teams represent governments, law enforcement agencies, academia, the private sector and other institutions.

21 Swiss Digital Foreign Policy Strategy 2021-2024: https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf

22 UN GGE Report 2015

23 Cf. ICT4Peace Paper: CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY (Geneva 2013), prepared with the support of the Swiss Ministry of Foreign Affairs: https://ict4peace.org/wp-content/uploads/2019/08/ICT4Peace-2013-Confidence-Building-Measure-And_Intern-Cybersecurity.pdf

Humanitarian engagement and assistance

Cyber warfare can cause loss of life and physical destruction that requires humanitarian assistance, as in traditional conflicts.

Should Switzerland, in the logic of assisting states under attack, envisage a more robust assistance, for example in the form of cyber rescue capacities?

Another conceivable form of assistance would be capacity building in cyber security. Especially for developing countries, the protection of critical ICT infrastructure is an enormous challenge, as they are increasingly dependent on digital resources. In addition to technical capacity building, the support could involve advice on legislation, regulatory measures and the development of effective cybersecurity strategies.[24] Within the UN framework, such forms of cooperation are supported and also demanded. However, practical cooperation is only at an initial stage. A complicating factor is that cybersecurity programs are not even eligible as official development assistance (ODA) according to the OECD/DAC criteria. Switzerland could work with like-minded countries to improve this. The experience with Covid-19 has made the importance of digital networking for developing countries well visible and prompted increased political awareness.

An effective form of cooperation and support worth examining is the establishment of Computer Emergency Response Teams (CERT), which are used to solve specific ICT security incidents. It is also important that this form of cooperation in the civilian sphere is not hindered by existing sanctions. As a neutral state, Switzerland is in a good position to address these concerns.

Norms of responsible behavior in cyberspace and strengthening international law

Switzerland bases its international relations on law and not on power. It has a particular interest in binding norms in cyberspace. This also applies in the event of armed conflicts that are fought in cyberspace.

24 Cf. International ICT4Peace Cyber Security Policy and Diplomacy Capacity Building Program https://ict4peace.org/wp-content/uploads/2021/01/Cybersecurity-Policy-and-Diplomacy-Capacity-Building-25-January-2021-2.pdf

Efforts to strengthen the international law are already underway. As in other areas of international humanitarian law, compliance with and enforcement of legal norms is particularly important. This could also be a worthwhile field of action for Switzerland with a political, legal and technical dimension.[25]

5. CONCLUSION

This discussion paper asks more questions than it answers. That is the purpose of a discussion paper. It is not about blueprints or hermetic statements, but about questions that hopefully generate comments and rebuttals. The timing is right as we face the return of great power rivalry and technological transformations. The European states, including neutral Switzerland, will be strongly affected by those developments.

The answers to the many questions raised, the concepts and doctrines will emerge as sequences of practical political decisions. This is precisely why it is necessary to deal with these questions in a timely and in-depth manner.

This text puts a strong emphasis on neutrality. Neutrality has been questioned with changes in international relations or weapons innovations. After the creation of the League of Nations and later the United Nations, with the advent of nuclear weapons or after the Cold War, the end of Swiss neutrality was announced. In fact, neutrality proved to be not only a safe political guide, but also a useful frame of reference for addressing the key issues we have to deal with in the context of conflicts and their prevention. This is certainly also true in the age of cyber warfare.

25 Cf. ICT4Peace work in support of Norms of Responsible State Behavior and Confidence Building Measure in Cyberspace: https://ict4peace.org/activities/norms-of-responsible-state-behavior/?load=all

About ICT4Peace Foundation

ICT4Peace is a policy and action-oriented international Foundation. The purpose is to save lives and protect human dignity through Information and Communication Technology. Since 2003 ICT4Peace explores and champions the use of ICTs and new media for peaceful purposes, including for peacebuilding, crisis management and humanitarian operations. Since 2007 ICT4Peace promotes cybersecurity and a peaceful cyberspace through inter alia international negotiations with governments, international organisations, companies and non-state actors.

The ICT4Peace project was launched with the support of the Swiss Government in 2003 with the publication of a book by the UN ICT Task Force on the practice and theory of ICT in the conflict cycle and peace building in 2005 and the approval of para 36 of the Tunis Commitment of the UN World Summit on the Information Society (WSIS) in 2005.

ICT4Peace on Twitter - www.twitter.com/ict4peace

ICT4Peace on Facebook - www.facebook.com/ict4peace

ICT4Peace official website: www.ict4peace.org

ICT4Peace additional publications: www.ict4peace.org/publications

ICT for peace foundation