ICT for peace foundation

POLICY BRIEF

# SCHWEIZER NEUTRALITÄT IM ZEITALTER DER CYBERKRIEGSFÜHRUNG

**Martin Dahinden**

**GENEVA 2021**

ICT4Peace Foundation

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

# SCHWEIZER NEUTRALITÄT IM ZEITALTER DER CYBERKRIEGSFÜHRUNG

**Martin Dahinden**

ICT for peace foundation

Diskussionspapier

# SCHWEIZER NEUTRALITÄT IM ZEITALTER DER CYBERKRIEGSFÜHRUNG

**Martin Dahinden**[1]

*Die Cyberkriegsführung ist eine neuartige und bedeutende Herausforderung für die schweizerische Neutralität. Ausgehend vom Neutralitätsrecht und der schweizerischen Neutralitätspolitik macht dieses Diskussionspapier eine Auslegeordnung zu wichtigen rechtlichen, politischen und konzeptionellen Fragestellungen. In erster Linie geht es um einen Beitrag zu einer beginnenden Debatte, aber auch um Handlungsoptionen, die sich für die Schweiz im veränderten Umfeld ergeben.*[2]

# EINLEITUNG

Die Fragen nach den Rechten und Pflichten neutraler Staaten im Cyberraum ist vielschichtig und kann keineswegs mit simplen Ableitungen aus dem geltenden Neutralitätsrecht und der herkömmlichen Neutralitätspolitik beantwortet werden.

Heute besteht ein breiter internationaler Konsens darüber, dass das Völkerrecht auch auf den Cyberraum anwendbar ist. Allerdings gehen die Rechtsauffassungen und politischen Haltungen weit auseinander, was das für die einzelnen völkerrechtlichen Normen konkret bedeutet. Diese Schlussfolgerung muss insbesondere aus den Beratungen gezogen werden, die während der vergangenen Jahre im Rahmen der

1 Martin Dahinden war Schweizer Botschafter in den USA, ist Mitglied des Stiftungsrates des Think-Tanks ICT4Peace und lehrt Sicherheitspolitik an der Universität Zürich

2 Für Kommentare und Inputs danke ich Sanija Ameti, Anne-Marie Buzatu, Serge Droz, Alain Modoux, Sara Pangrazzi, Daniel Stauffacher und Regina Surber

UNO geführt worden sind.[3] Das Verständnis des Problems ist dabei zwar vertieft worden; teilweise wurden auch gemeinsame Auffassungen formuliert. Zu einem eigentlichen Durchbruch in den kritischen Fragen und zu verbindlichen Normen ist es aber bisher nicht gekommen, weil sich politische Gegensätze nicht mit dem Formulieren von Rechtsauffassungen lösen lassen.

Auch das Neutralitätsrecht war direkt oder indirekt ein Thema in den internationalen Foren, die sich mit Cyberthemen befassen. Es ist offensichtlich, dass es auch im Zeitalter der Cyberkriegsführung Konflikte geben wird und Drittstaaten, die sich daran nicht beteiligen. Für diese Drittstaaten gelten die Rechte und Pflichten eines Neutralen. Wenig überraschend enthält deshalb etwa Tallinn Manual[4] ein eigenes Kapitel zur Neutralität.

Die dauernde Neutralität der Schweiz geht allerdings weit über diesen neutralitätsrechtlichen Kern hinaus. Die Schweiz befolgt auch in Friedenszeiten eine Politik, die glaubhaft macht, dass das Land in zukünftigen internationalen bewaffneten Konflikten neutral bleiben wird.

Der Cyberraum ist neuartig und weist viele Besonderheiten auf. Deshalb kann auch die Neutralitätspolitik der Schweiz für das Zeitalter der Cyberkriegsführung nicht

3 Vgl. Expertengruppe der Vereinten Nationen für Cybersicherheit (United Nations Group of Governmental Experts on Information Security UNGGE). Die UNGGE wurde 2004 vom Ersten Ausschuss der UNO Generalversammlung geschaffen mit dem Ziel zu beraten, wie Frieden und Sicherheit im Cyberraum durch Vertrauensbildenden Massnahmen und Normen für verantwortungsbewusstes Verhalten von Staaten, sowie Aufbau der notwendigen Kapazitäten gestärkt werden können. Siehe auch die parallel dazu 2018 von den Vereinten Nationen errichtete Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG). 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 unterstützt seit 2011 die UN GGE und UN OEWG Prozesse durch Expertenberichte, konkrete Vorschläge und Ausbildungsprogramme für Diplomaten und hohe Beamte. Ziel ist ein verantwortungsbewusstes Verhalten von Staaten, Vertrauensbildende Massnahmen, Normen, sowie der Aufbau der notwendigen staatlichen Kapazitäten (Vgl. Überblick: 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: Cambride University Press. Es handelt sich beim Tallinn Manual um eine wissenschaftliche Studie über die Anwendbarkeit des Kriegsvölkerrechts auf Cyberkonflikte und Cyberkriege (ius ad bellum; ius in bello). Das Tallinn Manual wurde zwischen 2009 und 2012 auf Einladung des NATO Cooperative Cyber Defence Center of Excellence von rund zwanzig Experten verfasst.

ohne weiteres aus den bestehenden Doktrinen zur Neutralitätspolitik abgeleitet werden, sondern erfordert vor allem sicherheitspolitische Denkarbeit.[5]

Die dauerhafte Neutralität ist darüber hinaus auch die Grundlage für die besondere Rolle der Schweiz in der Staatengemeinschaft. Weil sich aus der dauerhaften Neutralität Vorteile ergeben, hat die Schweiz ihren Neutralitätsstatus seit jeher als Pflicht verstanden, einen besonderen Beitrag zu Frieden und Sicherheit in der Welt zu leisten. Dazu gehören unter anderem das humanitäre Engagement, die Bereitschaft Gute Dienste zu leisten, Anstrengungen zur Stärkung des Völkerrechts, das Engagement für Vertrauensbildende Massnahmen, Konfliktverhütung und Konfliktbewältigung. Wie kann und soll diese Rolle im Zeitalter der Cyberkriegsführung wahrgenommen werden?

# 1. NEUTRALITÄT ALS GRUNDSATZ DER SCHWEIZERISCHEN AUSSENPOLITIK

Die dauerhafte Neutralität ist ein zentraler Grundsatz des schweizerischen Staatsverständnisses und der schweizerischen Außenpolitik. Sie ist aber kein Staatsziel an sich, sondern dient der Sicherung der Unabhängigkeit des Landes und der Unverletzlichkeit des Staatsgebiets. Deshalb wird die Neutralität weder im Zweckartikel noch in den außenpolitischen Grundsätzen der Bundesverfassung erwähnt.[6]

Das Neutralitätsrecht wurde in den Haager Abkommen vom 18. Oktober 1907[7] kodifiziert und ist heute Teil des Völkergewohnheitsrechts. Es legt die Rechte und die Pflichten eines neutralen Staates fest.

---

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

6 Dieser Abschnitt orientiert sich an der offiziellen Darstellung der Neutralität durch das Eidg. Departement für auswärtige Angelegenheiten EDA. Damit soll für die Argumentation ein klarer Bezug zur bestehenden Neutralitätsauffassung gemacht werden.

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

Das wichtigste dieser Rechte ist die Unverletzlichkeit des Staatsgebiets.

Die wichtigsten Pflichten des neutralen Staates sind,

- an keinen internationalen bewaffneten Konflikten teilzunehmen;
- die eigene Selbstverteidigung sicherzustellen;
- alle Kriegsparteien in Hinblick auf den Export von Rüstungsgütern gleich zu behandeln;
- den Kriegsparteien keine Truppen oder Söldner zur Verfügung zu stellen;
- den Kriegsparteien das eigene Staatsgebiet nicht zur Verfügung zu stellen.

Das Neutralitätsrecht bezieht sich auf Konflikte zwischen Staaten. Auf militärische Operationen, die vom Sicherheitsrat der Vereinten Nationen autorisiert wurden, ist es nicht anwendbar. Wie alle Staaten haben auch neutrale Staaten das Recht auf Selbstverteidigung im Falle eines bewaffneten Angriffes.

Die Neutralitätspolitik besteht in der Gesamtheit der Maßnahmen, die ein neutraler Staat ergreift, um seinen Neutralitätsstatus glaubwürdig zu machen. Die konkrete Ausgestaltung der Neutralitätspolitik hängt stark vom internationalen Umfeld ab und von dessen Beurteilung. Entsprechend ist die Neutralitätspolitik im Verlaufe der Zeit erheblichen Veränderungen unterworfen. Die Neutralitätspolitik führt zu einer eigentlichen Praxis, die letztlich weit über den rechtlichen Kern der Neutralität hinaus reicht.

# 2. HERAUSFORDERUNG CYBERRAUM

Informations- und Kommunikationstechnologien (ICT) beinhalten ein beispielloses Potenzial für die gesellschaftliche und wirtschaftliche Entwicklung, zugleich aber auch grosse Risiken für den Frieden und die internationale Sicherheit. Inzwischen haben viele Staaten ICT-Kapazitäten für militärische Zwecke aufgebaut und bauen sie weiterhin in grossem Umfang aus. Damit ist zusätzlich zum Land-, See- und Luftkrieg eine neue, vierte Dimension der Kriegsführung entstanden.

Drei Haupttypen von Cyberoperationen sind in diesem Zusammenhang zu unterscheiden:

1. **Computer Network Exploitations** (CNE) sind Operationen, die in fremde Netzwerke eindringen, um Informationen zu entwenden, idealerweise ohne Spuren zu hinterlassen.

2. **Computer Network Attacks** (CNA) sind Angriffe auf Systeme, um sie zu stören, beschädigen oder sogar zu vernichten, einschliesslich der gespeicherten Informationen. Es handelt sich bei den CNA's um die grössten Risiken, vor allem wenn sie sich gegen kritische Infrastruktur richten.

3. **Information Operations** (IO) beeinflussen Meinungen in einem fremden Staat zugunsten der eigenen Absichten.[8]

Typischerweise sind Cyberangriffe Teil einer hybriden Kriegsführung, d.h. sie treten kombiniert mit regulären und irregulären, mit symmetrischen und asymmetrischen, militärischen und nichtmilitärischen, offenen und verdeckten Kampfformen auf.[9] Bei Cyberoperationen ist es oft schwierig, die Urheber von Angriffen zu identifizieren (Zuordnung). Schwierig ist es auch zu bestimmen, bei welchen Aktivitäten und ab welcher Intensität es sich um einen Angriff bzw. einen bewaffneten Konflikt handelt. Oft ist es sogar schwierig festzustellen, ob überhaupt ein Angriff vorliegt oder ob es sich um einen Kollateralschaden handelt.[10]

Im herkömmlichen Neutralitätsrecht spielt das Staatsgebiet für die Rechte und Pflichten des neutralen Staates eine wichtige Rolle. Auch im Zeitalter der Cyberkriegsführung ist das Staatsgebiet relevant, denn nationale Rechtsordnungen und die faktische Kontrolle haben weiterhin eine geografische Dimension. Der physisch schwer fassbare

8 Vgl. Meyer, Paul, Stauffacher, Daniel (2021): Neue Zürcher Zeitung, 11. Februar 2021

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

10 ICT Operationen werden auch für terroristische Zwecke oder von kriminellen Organisationen eingesetzt. Sie sind aber nicht Gegenstand dieses Diskussionspapiers, das auf die Neutralitätsaspekte fokussiert. 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

Cyberraum führt allerdings zu einer Komplexität, welche die bisherigen Erfahrungen übersteigt.

Es ist zweckmässig den Cyberraum, das Internet als globales öffentliches Gut aufzufassen, ohne dass damit die Souveränität der Staaten in Bezug auf Einrichtungen, Personen, geistiges Eigentum usw. aufgehoben wird. Eine solche Sichtweise ist nicht verbreitet, wahrscheinlich weil sie ein politisch-ökonomisches Konzept (global commons) mit rechtlichen Kategorien verknüpft.

Zur Komplexität des Cyberraumes und der Cyberkriegsführung trägt auch bei, dass im Gegensatz zur herkömmlichen Kriegsführung grundsätzlich jeder Zugriff erhalten kann und weil die im humanitären Völkerrecht fundamentale Unterscheidung zwischen Zivilpersonen und Kombattanten besonders unklar ist.

# 3. NEUTRALITÄT IM CYBERRAUM

In den folgenden Abschnitten geht es um die Neutralität im Cyberraum in rechtlicher und politischer Hinsicht, es geht um einen Überblick, um Fragen und - soweit möglich - auch um Antworten. Die Gliederung folgt den wichtigsten Rechten und Pflichten für Neutrale, wie oben genannt.

## Unverletzlichkeit des Staatsgebiets

Das wichtigste Recht eines neutralen Staates ist die Unverletzlichkeit seines Staatsgebietes. Was aber heisst die Unverletzlichkeit des Staatsgebiets im Zusammenhang mit Cyberoperationen? Geht es um physische Wirkungen (Schäden an Menschen und Objekten)? Geht es auch um die Infrastruktur und die Funktionsfähigkeit internetbasierter Instrumente? Geht es um einen umfassenden Schutz des digitalen Raums, der unter der Kontrolle und der rechtlichen Zuständigkeit eines Staates steht?

Die Unverletzlichkeit ihres Staatsgebiets steht selbstverständlich allen Staaten zu, nicht nur den neutralen. Weil sich diese Frage für alle gleich oder ähnlich stellt,

sind die internationalen Beratungen in diesem Bereich auch von unmittelbarer von Bedeutung für die Schweiz.

## Selbstverteidigung bei Cyberangriffen

Gemäss Artikel 51 der UNO Charta haben Staaten, die angegriffen werden, das Recht auf Selbstverteidigung. Es handelt sich dabei um eine Ausnahme vom allgemeinen Gewaltverbot der UNO Charta.

Die Frage, ab welcher Schwelle ein Angriff ein Ausmass erreicht, das den angegriffenen Staat dazu legitimiert mit digitalen oder auch kinetischen Mitteln gegen einen Angreifer vorzugehen, ist indessen umstritten.[11] Auch dabei geht es nicht nur um eine rechtliche Einordnung, sondern um letztlich politische Entscheide, wann und mit welchen Mitteln das Recht auf Selbstverteidigung in Anspruch genommen wird. Entsprechende Doktrinen können eine dissuasive Wirkung haben oder in eine Eskalation hineinführen usw.

Zwar betrifft auch diese Problemstellung sämtliche Staaten. Für den neutralen Staat ist sie aber von besonderer Bedeutung, weil es auch darum geht, ob ein Cyberangriff «nur» die Neutralität verletzt und ab welcher Intensität der neutrale Staat selber zur Partei in einem bewaffneten Konflikt wird.

## Kooperation in den Bereichen Schutz und Abwehr

Die Kooperation mit anderen Staaten in den Bereichen Schutz und Abwehr ist für neutrale Staaten zulässig, aber ein heikles Feld, weil Abhängigkeiten entstehen können und die Glaubwürdigkeit der Neutralität für den Fall eines Konflikts beeinträchtigt werden kann. Der Beitritt zu einem Verteidigungsbündnis ist auf jeden Fall mit der Neutralität nicht vereinbar. Erfahrungsaustausch, Ausbildungs- und Rüstungszusammenarbeit usw. sind aber durchaus zulässig.

Wie steht es damit im Cyberbereich? Welche konkreten Formen der Zusammenarbeit sind zulässig, ohne dass Ungewissheit entsteht, ob der neutrale Staat im Falle

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

eines Konfliktes tatsächlich neutral sein kann und will? Gibt es rechtliche Grenzen (Vereinbarungen usw.) oder Grenzen sachlicher Art (gemeinsame Infrastruktur, Interoperabilität usw.)?

Die UNO empfiehlt, dass Staaten unterstützt werden, falls ihre Infrastruktur einem Cyberangriff ausgesetzt wird.[12] Unter welchen Voraussetzungen ist eine Unterstützung auch durch einen neutralen Staat unbedenklich (ähnlich der humanitären Hilfe)? Wann wird die Hilfeleistung zur neutralitätsrechtlich unzulässigen Unterstützung einer Konfliktpartei?

## Nichtteilnahme an bewaffneten Konflikten

Dem neutralen Staat ist es untersagt, an bewaffneten Konflikten teilzunehmen. Selbstverständlich ist das auch der Fall, wenn ein Konflikt ganz oder teilweise mit digitalen Mitteln ausgefochten wird.

Auf den ersten Blick scheint diese Bestimmung sehr unmissverständlich zu sein. Allerdings setzt das voraus, dass klar ist, ob ein bewaffneter Konflikt überhaupt vorliegt. Die Thematik führt zurück in die Fragestellungen nach der Kriegsschwelle, der Zuordnung von Cyberangriffen und in die Problematik der hybriden Kriegsführung.

## Sicherstellen der Selbstverteidigung

Die Bestimmung, dass neutrale Staaten ihre eigene Selbstverteidigung sicherzustellen haben, dient der Glaubwürdigkeit und der Berechenbarkeit der Neutralität.

Was bedeutet eine solche Verpflichtung im Zeitalter der Cyberkriegsführung? Sie bedeutet im Analogieschluss zur konventionellen Kriegsführung, dass der neutrale Staat verpflichtet ist, seine Infrastruktur derart zu schützen, dass sie von Konfliktparteien nicht verwendet werden kann. Ein neutraler Staat, der sich nicht schützt bzw. die zumutbaren Schutzmaßnahmen unterlässt, würde deshalb den Verpflichtungen eines neutralen Staates nicht nachkommen. Die UNO fordert zudem

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)

unabhängig von der Thematik der Neutralität, dass die Staaten Schutzmaßnahmen gegen Cyberangriffe umsetzen.[13]

Welche konkreten Vorkehrungen sind aber erforderlich? Was ist zumutbar? Handelt es sich um passive Schutzmaßnahmen (Firewalls, Zugriffsverweigerung auf Infrastruktur, Abwehr von Schadprogrammen usw.)?[14] Wie steht es mit Bedrohungen, die nicht auf dem eigenen Territorium stattfinden, beispielsweise mit einer Phishing-Seite, die genutzt wird, um Zugangsdaten zu sammeln? Ist eine abschreckende offensive Cyberkapazität notwendig und zulässig, um Cyberoperationen zu verhindern?

Das führt zur heiklen Frage, in welchem Ausmaß der neutrale Staat selber über offensive Cyberkapazitäten verfügen soll, um präventiv und präemptiv wirken zu können. Neutralitätspolitisch könnte Zurückhaltung geboten sein. Allerdings sprechen mindestens zwei Argumente auch für eine offensive Cyberkapazität. Erstens ist es schwer vorstellbar, dass wirksame Schutzmaßnahmen gegen Cyberangriffe aufgebaut werden können, ohne selber über entsprechende Fähigkeiten zu verfügen. Zweitens kann der neutrale Staat nicht ausschließen, dass er selber angegriffen wird und unter Artikel 51 der UNO-Charta vom Recht auf Selbstverteidigung Gebrauch machen will.

## Gleichbehandlung aller Kriegsparteien in Hinblick auf den Export von Rüstungsgütern

Beim Export von Rüstungsgütern (Geräten, Technologien) hat der Neutrale alle Kriegsparteien gleich zu behandeln. Es geht nicht um ein Verbot, sondern um ein Diskriminierungsverbot. Die der schweizerischen Kriegsmaterialausfuhrpolitik geht es allerdings bei weitem nicht nur um eine Überprüfung der Vereinbarkeit mit dem Neutralitätsrecht und der Neutralitätspolitik, sondern um weitreichende außenpolitische Zielsetzungen (Menschenrechte, Entwicklungspolitik usw.).[15] Damit stellt sich konsequenterweise auch die Frage, wie die Ausfuhr von Gütern

13 UN GGE Report 2015

14 Vgl. Basismassnahmen der Cyber-Sicherheit des deutschen Bundesamtes für Sicherheit in der Informationstechnik: https://docplayer.org/114578396-Basismassnahmen-der-cyber-sicherheit.html

15 Artikel 5 Kriegsmaterialverordnung (https://www.fedlex.admin.ch/eli/cc/1998/808_808_808/de)

und Technologien gehandhabt werden soll, die für die für die Cyberkriegsführung bestimmt sind.

Geräte und Technologien, die für die Cyberkriegsführung eingesetzt werden, sind weitestgehend Dual-use-Güter, also Güter, die für zivile, wie auch für militärische Zwecke einsetzbar sind. Sie haben in dieser Hinsicht ähnliche Charakteristika wie die Dual-use-Güter der Raketentechnologie oder im Nuklear-, Biologie und Chemiebereich, wo internationale Exportkontrollregimes bestehen. Die Schweiz befürwortet generell multilaterale Kontrollmaßnahmen gegen die unerwünschte Verbreitung von Dual-use-Gütern. Ein solches Kontrollregime gibt es für den Cyberbereich nicht. Gewisse Geräte und Technologien werden im Rahmen des Wassenaar-Arrangements kontrolliert. Die Aussicht, dass in absehbarer Zeit wirksame in diesem oder in einem anderen Rahmen multilaterale Exportkontrollen entstehen, ist gering. Wahrscheinlich ist, dass die USA, China und die EU unilaterale Kontrollen einführen und Drittstaaten wie die Schweiz unter Druck setzen, was neutralitätspolitisch und im Konfliktfall auch neutralitätsrechtlich heikel sein kann.[16]

## Sanktionen

Der UNO Sicherheitsrat ist befugt, Sanktionen zu ergreifen, die für sämtliche Staaten rechtlich bindend sind. Auch können Staaten allein oder gemeinsam mit anderen Sanktionen ergreifen, um aussenpolitische Ziele zu verfolgen, beispielsweise die Einhaltung des Völkerrechts oder die Respektierung der Menschenrechte. Solche Sanktionen haben nur in seltenen Fällen einen direkten Bezug zum Neutralitätsrecht. Allerdings können sie, ähnlich wie die Exportkontrollen, die Glaubwürdigkeit des neutralen Staates beeinträchtigen. Das trifft auch auf Sanktionen zu, die als Massnahme gegen Cyberoperationen ergriffen würden.

16 Vgl. Holzer, Patrick Edgar (2020): Das Güterkontrollgesetz (Definitionen im Güterkontrollgesetz. In: Cottier, Thomas, Oesch, Matthias (Hrsg.) Schweizerisches Bundesverwaltungsrecht Band XI, Allgemeines Aussenwirtschafts- und Binnenmarktrecht. Basel: Helbing Lichtenhahn Verlag, 147-230. Publikationen des Wassenaar Arrangements: https://www.wassenaar.org/de/

## Verbot den Kriegsparteien Truppen oder Söldner zur Verfügung zu stellen

Neutrale Staaten dürfen Kriegsparteien keine Truppen oder Söldner zur Verfügung stellen und dürfen keine Rekrutierung auf dem eigenen Staatsgebiet zulassen.

Wie hat sich ein neutraler Staat gegenüber privaten Firmen und Personen zu verhalten, die in ihrem Hoheitsgebiet im Bereich Cybersicherheit aktiv sind und Technologien oder Dienstleistungen für Cyberoperationen anbieten? In diesem Bereich gehen die neutralitätsrechtlichen Bestimmungen teilweise über das Diskriminierungsverbot hinaus und verlangen eigentliche Verbote. Es handelt sich um eine analoge Problematik zu den privaten Sicherheitsfirmen. Deshalb lohnt es sich, das Thema in Analogie zum Montreux-Dokument bzw. Montreux Prozess zu vertiefen - und zwar nicht nur unter dem Aspekt der menschlichen Sicherheit, sondern auch unter dem Aspekt der Neutralität.[17]

Klärungsbedarf besteht auch in Bezug auf Begriffe wie Soldat und Söldner. Was bedeuten sie im Kontext der Cyberkriegsführung? Handelt es sich dabei ausschließlich um Menschen, die digitale Ressourcen als Kampfmittel einsetzen oder fallen auch Bots, Bot-Farmen usw. unter diesen Begriff? Und wie steht es um die staatliche Verantwortlichkeit in diesem Zusammenhang?

## Verbot den Kriegsparteien das eigene Staatsgebiet zur Verfügung zu stellen

Neutralen ist es untersagt, den Kriegsparteien ihr Staatsgebiet zur Verfügung zu stellen. Diese Verpflichtung ist ein Verbot, das über den Gleichbehandlungsgrundsatz (Diskriminierungsverbot) hinaus geht.

Das Haager Abkommen vom 18. Oktober 1907 enthält Bestimmungen über den drahtlosen Funkverkehr. Demnach dürfen neutrale Staaten keine solchen Anlagen auf ihrem Territorium zulassen, wenn diese dem Verkehr zwischen den Streitkräften

17 Siehe EDA, Montreux Dokument: https://www.eda.admin.ch/eda/de/home/aussenpolitik/voelkerrecht/humanitaeres-voelkerrecht/private-sicherheitsunternehmen/montreux-dokument.html)

kriegsführender Staaten dienen (Artikel 3). Hingegen sind sie nicht verpflichtet, den Kriegsführenden jeglichen drahtlosen Funkverkehr, der über ihr Territorium abgewickelt wird, zu untersagen (Artikel 7).[18]

Im Analogieschluss würde das wohl bedeuten, dass der Neutrale die Nutzung seine Infrastruktur (Server, Kommunikationsnetze usw.) für die Cyberkriegsführung anderer Staaten nicht zulassen darf. Er wäre aber selbst im Falle eines bewaffneten Konfliktes nicht dazu verpflichtet, sämtliche (also auch die zivile) Nutzung von ICT Kapazität zu verhindern. Eine solche Abgrenzung ist nicht einfach und bedarf einer Klärung, man denke etwa an Informationsoperationen im Rahmen der hybriden Kriegsführung, wo es nicht fassbar ist, über welche ICT-Infrastruktur Informationen verbreitet werden.

Anzumerken ist in diesem Zusammenhang, dass die UNO Experten verlangen, dass die Staaten nicht wissentlich zulassen, dass ihr Hoheitsgebiet für völkerrechtswidrige Handlungen unter Verwendung von ICT genutzt wird.[19]

# 4. DENKANSTÖSSE FÜR FRIEDEN UND MEHR SICHERHEIT IM CYBERRAUM

Die schweizerische Neutralitätspolitik prägt die schweizerische Außenpolitik weit über den Kern des Neutralitätsrecht und über die Neutralitäts-Doktrinen hinaus. Sie ist verankert in historischen Erfahrungen und der politischen Kultur der Schweiz. Es gibt keinen Grund, diese Traditionen zu verlassen, weil neue Formen der Konfliktaustragung auftreten. Im Gegenteil: es ist zu überlegen, wie Beiträge für Frieden und Sicherheit im Zeitalter der Cyberkriegsführung geleistet werden können.

Das Spektrum möglicher Aktivitäten groß. In den folgenden Abschnitten geht es keineswegs darum, alle möglichen Tätigkeitsbereiche auf den Cyberraum hin zu

18 Abkommen betreffend die Rechte und Pflichten der neutralen Mächte und Personen im Falle eines Landkriegs, Artikel 3 und Artikel 7: https://www.fedlex.admin.ch/eli/cc/26/499_376_481/de

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).

deklinieren, sondern um einige knapp formulierte Hinweise auf überlegenswerte Pisten.

## Gute Dienste

Neutrale Staaten eignen sich besonders, um Gute Dienste zu erbringen. Darunter werden heute alle möglichen Hilfeleistungen für Dritte verstanden (Schutzmachtmandaten, Gastgeber für internationale Konferenzen und Organisationen, Factfinding, Beiträge zur friedlichen Streitbeilegung usw.).

Die finanzielle Unterstützung von Factfinding Aktivitäten (Attribution von Cyber-Zwischenfällen bis hin zum Fakten-Überprüfung im Zusammenhang mit Informationsoperationen) sind ein Tätigkeitsfeld, das sich in der Tradition der Guten Dienste bewegt. Ebenso die Unterstützung von Initiativen wie FIRST (Forum for Incident Response and Security Teams).[20]

Auch die Förderung des Gouvernanzstandorts Schweiz und die Anstrengungen, Genf zu einem Hub für die Zusammenarbeit im digitalen Bereich zu machen, gehören in diesen Rahmen.[21] Dazu können Synergien zu den bereits vorhandenen multilateralen Strukturen genutzt werden.

## Vertrauensbildende Maßnahmen

Vertrauensbildende Maßnahmen haben ein großes Potenzial zur Vermeidung und Beschwichtigung von Konflikten. Vertrauensbildende Maßnahmen werden oft im Rahmen von internationalen Abkommen oder internationalen Organisationen erbracht. Ein neutraler Staat kann dabei wirkungsvoll unterstützen, indem er mit seiner Glaubwürdigkeit Vorschläge einbringt und gegebenenfalls auch selber Maßnahmen zur Vertrauensbildung umsetzt.

---

20 Das «Forum for Incident Response and Security Teams» (FIRST) ist ein internationaler Zusammenschluss von einzelnen CERTs, die zusammenarbeiten, um technische und sicherheitsrelevante Informationen auszutauschen. Es umfasst über 220 Mitglieder aus 42 Ländern. Die Incident-Response-Teams der Mitglieder vertreten Regierungen, Strafverfolgungsbehörden, Hochschulen, den Privatsektor und weitere Institutionen.

21 Strategie Digitalaussenpolitik 2021-2024: https://www.newsd.admin.ch/newsd/message/attachments/63601.pdf

Während der Beratungen im UNO-Rahmen ist ein Konsens erzielt worden, dass eine stärkere Zusammenarbeit und mehr Transparenz geeignet sind, Konfliktrisiken zu reduzieren. Dabei sind auch freiwillige Vertrauensbildende Maßnahmen identifiziert worden. Auch wenn die Staaten die Hauptverantwortung tragen, ist es wichtig, dass auch der Privatsektor, die Wissenschaft und die Zivilgesellschaft in das Erarbeiten von Lösungen einbezogen wird.[22] Dazu kann die Schweiz mit ihrem direkten und unkomplizierten Umgang mit diesen Interessengruppen einen besonderen Beitrag leisten, wie sie es beispielsweise im Bereich der Vertrauensbildenden Massnahmen für einen friedlichen Cyberspace getan hat.[23]

## Humanitäres Engagement und Hilfeleistung

Die Cyberkriegsführung kann Opfer an Menschenleben und physische Zerstörungen verursachen, die humanitäre Hilfe erfordert, wie in herkömmlichen Konflikten.

Ist es angezeigt, in der Logik der Unterstützung angegriffener Staaten eine weitergehende Hilfeleistung ins Auge zu fassen, beispielsweise in Form von Cyber Rescue Kapazitäten?

Eine denkbare weitere Form der Hilfeleistung wäre die Unterstützung beim Aufbau von Cybersicherheits-Kapazitäten. Vor allem für Entwicklungslänger ist der Schutz von kritischer ICT-Infrastruktur eine enorme Herausforderung, obwohl auch sie zunehmend abhängig sind von digitalen Kapazitäten. Neben dem Aufbau von technischen Fähigkeiten geht es dabei auch um Beratung bei der Gesetzgebung, um Regulierungsmassnahmen und um die Entwickelung wirksamer Strategien der Cybersicherheit.[24] Im Rahmen der UNO werden solche Formen der Zusammenarbeit unterstützt und auch gefordert. Allerdings befindet sich die Zusammenarbeit erst in einer Anfangsphase. Erschwerend ist, dass Programme der Cybersicherheit gemäss den OECD/DAC-Kriterien nicht einmal als offizielle Entwicklungshilfe (ODA)

22 UN GGE Report 2015

23 Vgl. ICT4Peace Papier: CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY (Geneva 2013), erstellt mit Unterstützung des EDA. https://ict4peace.org/wp- content/uploads/2019/08/ICT4Peace-2013-Confidence-Building-Measure-And_Intern-Cybersecurity.pdf

24 Vgl. 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

anrechenbar sind. Die Schweiz könnte sich zusammen mit gleichgesinnten Staaten für eine Verbesserung einsetzen. Die Erfahrungen mit Covid-19 haben die Bedeutung der digitalen Vernetzung auch für Entwicklungsländer gut sichtbar gemacht und die Sensibilität dafür erhöht.

Eine wirkungsvolle und prüfenswerte Form der Zusammenarbeit und Unterstützung ist der Aufbau von Computer Emergency Response Teams (CERT), die bei der Lösung konkreter ICT-Sicherheitsvorfällen zum Einsatz kommen. Wichtig ist auch, dass diese Form der Zusammenarbeit im zivilen Bereich nicht von Sanktionen behindert wird. Auch für diese Anliegen ist die Schweiz als neutraler Staat in einer guten Ausgangslage.

## Normen im Cyberraum und Stärkung des Völkerrechts

Die Schweiz stützt sich in ihren internationalen Beziehungen auf das Recht und nicht auf Macht ab. Sie hat ein besonderes Interesse an verbindlichen Normen im Cyberraum. Das gilt auch für den Fall bewaffneten Konflikten, die im Cyberraum ausgetragen werden.

Anstrengungen zur Stärkung des Rechts laufen bereits auf internationaler Ebene. In diesem Bereich geht es, wie in anderen Bereichen des humanitären Völkerrechts, besonders auch um die Einhaltung und Durchsetzung von Rechtsnormen. Auch das ist ein lohnenswertes Wirkungsfeld für die Schweiz, das eine politische, rechtliche und technische Dimension aufweist.[25]

# 5. SCHLUSS

Dieses Diskussionspapier stellt mehr Fragen als es beantwortet. Das ist der Zweck eines Diskussionspapiers. Es geht nicht um Blaupausen oder hermetische Aussagen, sondern um Fragen, die hoffentlich Kommentare und Widerrede hervorbringen. Dazu ist der Zeitpunkt richtig wegen der Rückkehr der Großmacht-Rivalität und der

25 Vgl. Arbeiten von ICT4Peace zur Unterstützung von Norms of Responsible State Behaviour and Confidence Building Measure in Cyberspace: https://ict4peace.org/activities/norms-of-responsible-state-behavior/?load=all

absehbaren technologischen Umbrüche. Die europäischen Staaten, auch die neutrale Schweiz, werden von dieser Entwicklung stark betroffen sein.

Die Antworten auf die vielen aufgeworfenen Fragen, die tragenden Konzepte und Doktrinen werden sich als Abfolgen praktischer politischer Entscheide ergeben. Gerade deshalb ist es erforderlich sich mit diesen Fragestellungen rechtzeitig und vertieft zu befassen.

Das Diskussionspapier hat einen starken Fokus auf die Neutralität. Seit langem besteht auch die Vorstellung, dass politische und waffentechnische Neuerungen die Neutralität zu einem Relikt machen. Mit der Gründung des Völkerbunds und später der Vereinten Nationen, mit dem Aufkommen der Nuklearwaffen oder dem Ende des kalten Krieges wurde das Ende der schweizerischen Neutralität prognostiziert. Tatsächlich hat sich die Neutralität nicht nur als sicherer politischer Leitfaden erwiesen, sondern auch als nützliches Denkraster, das in die Kernfragen hineinführt, um die wir uns im Zusammenhang mit Konflikten und ihrer Vermeidung kümmern müssen. Das trifft auch auf das Zeitalter der Cyberkriegsführung zu.

## 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