Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für auswärtige Angelegenheiten EDA
Direktion für Völkerrecht (DV)

Schweizer Positionspapier: Die Anwendung des Völkerrechts im Cyberraum

Annex UN GGE Cybersicherheit 2019/2021

Einleitung

Bei den Arbeiten der UNO-Gruppe von Regierungsexperten für Entwicklungen im Bereich der Informations- und Telekommunikationstechnologien im Kontext der internationalen Sicherheit 2019/2021 (UN GGE) stehen für die Staaten primär die sicherheitspolitische Dimension des digitalen Raums (Cybersicherheit) und die in diesem Rahmen geltenden völkerrechtlichen Vorgaben im Vordergrund.[1] Mit dem Begriff Cyberraum ist damit derjenige Teil des digitalen Raums gemeint, der die sicherheitspolitische Dimension betrifft. Die Position geht einerseits auf Fragen des Allgemeinen Völkerrechts inklusive der Menschrechte ein (Teil I) und setzt andererseits ein besonderes Augenmerk auf Fragen des Humanitären Völkerrechts (Teil II).

Die Schweiz setzt sich für den Aufbau und die Gewährleistung eines offenen, freien, sicheren und friedlichen Cyberraums sowie für die Förderung der Anerkennung, Einhaltung und Durchsetzung des Völkerrechts in diesem Raum ein.[2] Es liegt im gemeinsamen Interesse aller Staaten, sicherzustellen, dass der Cyberraum rechtsstaatlich geregelt und friedlich genutzt wird. Aus Sicht der Schweiz findet das Völkerrecht im Cyberraum Anwendung. Die Schweiz begrüsst daher den von allen Staaten in der UNO-Generalversammlung bestätigten[3] Konsens bisheriger UN GGEs, der besagt, dass das Völkerrecht und insbesondere die UNO-Charta in ihrer Gesamtheit im Cyberraum Anwendung finden.[4] Sie begrüsst ebenso die Bestätigung dieses Konsens im Bericht der OEWG 2019/2021 vom 18. März 2021.[5]

Die Schweiz ist der Ansicht, dass nationale staatliche Positionen einen wichtigen Beitrag zur weiteren Konkretisierung der Anwendung des Völkerrechts im Cyberraum leisten. Die Schweizer Position gibt einen Überblick und ist weder abschliessend noch vollständig.

---

1 Zum Engagement der Schweiz für das internationale Regelwerk im digitalen Raum im Allgemeinen siehe Strategie Digitalaussenpolitik (2021-2024) und namentlich den Anhang 4 zum internationalen Regelwerk (https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf).

2 Siehe Aussenpolitischen Strategie der Schweiz (2020-2023) Ziel 4.4 und Strategie Digitalaussenpolitik der Schweiz (2021-2024) Kapitel 4.3.

3 Resolution A/70/237.

4 Siehe Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report (2013 report, UN Doc. A/68/98, para.19; 2015 report (UN Doc. A/70/174), para. 24, para 28 c).

5 Siehe Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021 report, para 8, UN Doc. A/75/816.

Vielmehr braucht es auch weiterhin den engen zwischenstaatlichen Austausch im multilateralen Rahmen, um die konkrete Anwendung des Völkerrechts im Cyberraum weiter zu klären. Eine abschliessende völkerrechtliche Beurteilung eines Cybervorfalls ist immer erst im Lichte der konkreten Umstände möglich. Die im Folgenden dargelegten völkerrechtlichen Regeln müssen somit jeweils im Einzelfall ausgelegt und angewendet werden.

Von besonderer Bedeutung im Kontext der Cybersicherheit sind namentlich die im Folgenden dargestellten völkerrechtlichen Regeln.

I. Allgemeines Völkerrecht

1. Friedliche Streitbeilegung

Gemäss Art. 2 Abs. 3 und Art. 33 UNO-Charta sollen Streitigkeiten, welche die Wahrung des Weltfriedens und der internationalen Sicherheit gefährden können, friedlich beigelegt werden. Hierzu gehören diplomatische Verfahren, die Einsetzung von Schiedsgerichten oder die Anrufung des Internationalen Gerichtshofs (IGH). Als neutrales Land mit langjährigem Engagement und Erfahrung in der Bereitstellung von Guten Diensten setzt sich die Schweiz für die Einhaltung des Prinzips der friedlichen Streitbeilegung im Cyberraum ein, welches die friedliche Nutzung des Cyberraums als oberstes Ziel unterstreicht. Daher begrüsst die Schweiz, dass der UN GGE-Bericht 2015 und der Bericht der OEWG 2019/2021 das Prinzip der friedlichen Streitbeilegung als eines der zentralen Prinzipien der UNO-Charta bestätigt haben, welches auch im Cyberraum gilt. Streitigkeiten sind deshalb auch im Cyberraum grundsätzlich mit den Mitteln der friedlichen Streitbeilegung – und nicht mit unilateralen Massnahmen – beizulegen.

2. Souveränität

Die Souveränität ist ein grundlegendes völkerrechtliches Prinzip. Souveränität meint einerseits die Kompetenz von Staaten, ihre Rechtsordnung zu bestimmen, anzuwenden und durchzusetzen. Diese Kompetenz ist grundsätzlich territorial beschränkt. Im zwischenstaatlichen Verhältnis bedeutet Souveränität andererseits, dass Staaten unabhängig und gleichberechtigt nebeneinander existieren. Als Ausfluss der Souveränität hat jeder Staat Anspruch auf Achtung seiner territorialen Integrität und ist vor Einmischung geschützt.[6] Jeder Staat ist entsprechend verpflichtet, die Souveränität anderer Staaten zu beachten.[7] Bei der Souveränität handelt es sich um eine verbindliche, primäre Regel des Völkerrechts, deren Verletzung eine völkerrechtswidrige Handlung darstellt und bei gegebener Zurechnung die Staatenverantwortlichkeit begründet.

Die staatliche Souveränität gilt auch im Cyberraum.[8] Aufgrund der besonderen Bedingungen des Cyberraums, der keine klaren territorialen Grenzen kennt, stellt es eine besondere Herausforderung dar, das Prinzip der Souveränität zu konkretisieren. Dies betrifft vor allem auch die Frage, welche Staaten Jurisdiktion über digitale Daten oder einen Zugriff auf solche Daten haben. Zu berücksichtigen ist in diesem Kontext auch die Frage nach der legitimen Kontrolle über digitale Daten und der Berechtigung zum Zugriff auf Daten, welche je nach den

---

6 Island of Palmas Schiedsspruch, 1928, S. 838; Die Schweizerische Bundesverfassung anerkennt mit dem Begriff der Unabhängigkeit in Art. 2 Abs. 1 den völkerrechtlich souveränen Staat, dem die exklusive Zuständigkeit zur Rechtsetzung und zur Rechtsdurchsetzung auf seinem Hoheitsgebiet zusteht.

7 Military and Paramilitary Activities in and against Nicaragua, ICJ reports 1986, para 292.

8 UN GGE Bericht 2013, para. 20; UNGEE Bericht 2015, paras. 27, 28b).

Umständen auf einem anderen Territorium gespeichert sind oder deren geografische Lokalisierung nicht möglich ist. Im zwischenstaatlichen Verhältnis der Cybersicherheit lassen sich hingegen aus dem Prinzip der Souveränität verschiedene Schutzbereiche vor Cyberoperationen ableiten. Die Souveränität schützt dabei die Infrastruktur der Informations- und Kommunikationstechnik (IKT) auf dem staatlichen Hoheitsgebiet vor unbefugtem Eindringen und materiellen Schäden. Geschützt sind Computernetzwerke, Systeme und Software, die diese IKT Infrastrukturen unterstützen. Dies unabhängig davon, ob es sich um private oder öffentliche Infrastrukturen handelt.

Die Schweiz anerkennt, dass die Konkretisierung davon, was eine Verletzung dieses Schutzbereichs der Souveränität im Cyberraum darstellt, eine besondere Herausforderung darstellt und noch nicht abschliessend geklärt ist. Sie befürwortet, dass bei der Beurteilung zwei Kriterien zu beachten sind: Einerseits ist zu prüfen, ob ein Vorfall die territoriale Integrität eines Staates verletzt, andererseits, ob ein Vorfall eine Einmischung in eine inhärent staatliche Funktion oder eine widerrechtliche Aneignung einer solchen darstellt. Die exakte Interpretation dieser Kriterien ist eine Auslegungsfrage und Gegenstand von Diskussionen. Diskutiert werden unter anderem Fälle, in denen die Funktionalität einer Infrastruktur oder von mit ihr zusammenhängender Ausrüstung beschädigt oder eingeschränkt wird; Fälle, in denen Daten verändert oder gelöscht werden, die die Ausübung inhärent staatlicher Funktionen beinträchtigen, wie z.B. soziale Dienstleistungen; die Durchführung von Wahlen und Abstimmungen; die Erhebung von Steuern; und schliesslich Fälle, in denen Staaten durch koordinierten Einsatz legaler und illegaler Methoden im Cyberraum, wie z.B. Propaganda, Desinformation und verdeckte Aktionen von Nachrichtendiensten, versuchen, demokratische Entscheidungsprozesse in einem anderen Staat zu beeinflussen, zu stören oder zu verzögern. Im Einzelfall hängt die Beurteilung von der Art des Cybervorfalls und seinen Konsequenzen ab.

3. Interventionsverbot

Das Interventionsverbot fliesst aus dem Prinzip der souveränen Gleichheit der Staaten (Art. 2 Abs. 1 UNO-Charta) und gilt völkergewohnheitsrechtlich.[9] Unter Intervention wird die direkte oder indirekte Einmischung eines Staates mit Zwangsmitteln in die inneren oder äusseren Angelegenheiten eines anderen Staates verstanden. Erfasst sind Angelegenheiten für die der Staat die ausschliessliche Zuständigkeit inne hat (sog. domaine réservé). Zum Schutzbereich des Interventionsverbots zählen die inneren Angelegenheiten eines Staates, wie etwa die Wahl seines politischen, wirtschaftlichen, sozialen und kulturellen Systems, sowie die Gestaltung seiner Aussenpolitik. Im Unterschied zur Souveränitätsverletzung braucht es bei der verbotenen Intervention ein Zwangselement. Ein Staat versucht mit der Intervention, einen anderen Staat dazu zu bringen, anders zu agieren (Handlung oder Unterlassung), als er es ohne Zwang tun würde.[10] Damit ist die Schwelle einer Verletzung des Interventionsverbots bedeutend höher als diejenige einer Souveränitätsverletzung.

Das Interventionsverbot gilt auch im Cyberraum. Handlungen im Cyberraum können daher bei Vorliegen der entsprechenden Voraussetzungen neben einer Souveränitätsverletzung auch eine unzulässige politische oder wirtschaftliche Einmischung eines Staates in die inneren und äusseren Angelegenheiten eines anderen Staates darstellen und damit gegen das völkerrechtliche Interventionsverbot verstossen.[11] Die Abgrenzung zwischen noch

---

9 Friendly Relations Declaration, A/RES/2625 (XXV), 24. Oktober 1970; Military and Paramilitary Activities in and against Nicaragua, ICJ reports 1986, para 202.

10 Military and Paramilitary Activities in and against Nicaragua, ICJ reports 1986, para 202.

11 Erläuterungen Verordnung über die militärische Cyberabwehr (MCAV), SR 510.921.

erlaubter Einwirkung und verbotenem Zwang muss von Fall zu Fall beurteilt werden. Dies trifft insbesondere beim wirtschaftlichen Zwang zu. Ein solcher kann z.B. gegeben sein, wenn systemrelevante Unternehmen mittels einer Cyberoperation lahmgelegt werden. Um festzustellen, ob das Zwangselement bei Cyberoperationen erfüllt ist und somit eine Verletzung des Interventionsverbots vorliegt, ist eine Einzelfallprüfung notwendig.

4. Gewaltverbot und Selbstverteidigungsrecht

Eines der wichtigsten Grundprinzipien der UNO-Charta ist das Gewaltverbot (Art. 2 Abs. 4). Ausnahmen vom Gewaltverbot bestehen gemäss UNO-Charta, wenn der UNO-Sicherheitsrat die Anwendung von Gewalt autorisiert (Art. 42) oder die engen Voraussetzungen für die Ausübung des Selbstverteidigungsrechts erfüllt sind (Art. 51).

Das Gewaltverbot und das Selbstverteidigungsrecht gelten auch im Cyberraum. Für die Ausübung des Selbstverteidigungsrecht muss zunächst ein bewaffneter Angriff vorliegen. Gemäss Rechtsprechung des IGH stellt nicht jede Verletzung des Gewaltverbots einen bewaffneten Angriff dar, sondern nur die schwerste Form. Der bewaffnete Angriff muss daher eine gewisse Intensität und Wirkung erreichen.[12] Gemäss der Rechtsprechung des IGH muss ein bewaffneter Angriff nicht zwingend durch kinetische bzw. mechanische Mittel oder Waffen erfolgen, da die Mittel mit denen ein Angriff ausgeführt wird nicht das entscheidende Kriterium darstellen.[13] Gegen einen Cybervorfall, der aufgrund erheblicher Schäden an Personen (Verletzte bzw. Tote) oder erheblichen materiellen Schäden an Objekten in seiner Intensität und Wirkung einem kinetischen bewaffneten Angriff gleichkommt, darf sich ein Staat bei seiner Reaktion auf das Selbstverteidigungsrecht berufen. Es gibt keine verbindlichen, quantitativen und qualitativen Vorgaben, wann aufgrund der Intensität und Wirkung die Schwelle eines bewaffneten Angriffs erreicht ist. Diskutiert werden im Zusammenhang mit der Definition bewaffneter Angriffe im Cyberraum, Angriffe auf kritische Infrastrukturen (z.B. Atomkraftwerke, Stromnetze) mit der entsprechenden Intensität und Wirkung, d.h. mit erheblichen Schäden an Personen und/oder Objekten.

Bei der Auslegung des Gewaltverbots und des Rechts auf Selbstverteidigung bei Vorliegen eines bewaffneten Angriffs sind die Ziele der UNO-Charta zu beachten. Diese zielen auf die Wahrung und gegebenenfalls Wiederherstellung des Weltfriedens und der internationalen Sicherheit ab. Auch wenn ein bewaffneter Angriff vorliegt, sind nur Handlungen zulässig, die notwendig und verhältnismässig sind um den bewaffneten Angriff abzuwehren. Das Recht auf Selbstverteidigung gilt soweit als der UNO-Sicherheitsrat nicht die erforderlichen Massnahmen zur Wahrung des Weltfriedens und der internationalen Sicherheit getroffen hat (Art. 51 UNO-Charta). Überschreitet die Selbstverteidigung diesen Rahmen, wird sie selbst zur verbotenen Gewalt. Unterhalb der Schwelle des bewaffneten Angriffs hat der Staat ein Recht auf sofortige und verhältnismässige gewaltlose Gegenmassnahmen (siehe Ziff. 6.2).

5. Neutralität

Nach Ansicht der Schweiz gelten die Rechte und Pflichten neutraler Staaten im Rahmen internationaler bewaffneter Konflikte grundsätzlich auch im Cyberraum.[14] Besteht ein

---

12 Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para 195.

13 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para 39.

14 "The Court finds that as in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the

internationaler bewaffneter Konflikt, hat ein neutraler Staat die Pflicht, Verletzungen seiner Neutralität, etwa durch die Benutzung seines Territoriums durch eine Konfliktpartei, zu verhindern. Umgekehrt haben die Konfliktparteien die territoriale Unversehrtheit des Neutralen zu respektieren. Grundsätzlich folgt daraus, dass die Konfliktparteien Cyberoperationen im Zusammenhang mit dem Konflikt nicht von Installationen auf dem Territorium eines neutralen Staates oder von solchen, die unter dessen exklusiver Kontrolle stehen, ausführen dürfen.[15] Es ist ihnen ebenfalls verboten, die Kontrolle über Computersysteme des neutralen Staates zu übernehmen, um solche Operationen auszuführen.[16]

Den auf das Territorium bezogenen Rechten und Pflichten des Neutralen sind im Cyberraum aufgrund seiner globalen grenzüberschreitenden Natur auch Grenzen gesetzt. Während der Luftraum für spezifische Flugobjekte gesperrt werden kann, ist dies bei Datenverkehr im Internet nicht auf die gleiche, gezielte Weise möglich. Schliesslich werden Daten nicht nur über terrestrische Kabel, sondern auch über Satelliten übertragen, die sich im Weltraum und damit ausserhalb des Anwendungsbereichs des Neutralitätsrechts befinden. Diese Elemente sind zu berücksichtigen, wenn die Rechte und Pflichten des Neutralen auf den Cyberraum angewandt werden.

Es ist den Kriegsparteien grundsätzlich nicht erlaubt, durch ihre über Computernetze durchgeführten Kampfhandlungen die Datennetze von Neutralen zu schädigen. Ein neutraler Staat darf Konfliktparteien weder durch Truppen noch durch eigene Waffen unterstützen. Übertragen auf militärische Cyberaktivitäten im Rahmen von internationalen bewaffneten Konflikten bedeutet dies, dass ein neutraler Staat die Nutzung seiner militärisch kontrollierten Systeme und Netzwerke durch eine Konfliktpartei verhindern muss. Militärische Netzwerke sind grundsätzlich abgeschirmt und nicht allgemein zugänglich.

6. Staatenverantwortlichkeit

Die Regeln zur Staatenverantwortlichkeit bilden grundsätzlich Völkergewohnheitsrecht ab und sind im Entwurf der Völkerrechtskommission weitgehend wiedergegeben.[17] Diese Regeln sind auch auf Cybervorfälle anwendbar. Sie sehen vor, dass jedes völkerrechtswidrige Handeln eines Staates dessen völkerrechtliche Verantwortlichkeit zur Folge hat und einen Anspruch auf vollständige Wiedergutmachung begründet. Voraussetzung ist dabei, dass das Handeln einem Staat rechtlich zurechenbar ist (Attribution) und eine völkerrechtswidrige Handlung, d.h. die Verletzung einer völkerrechtlichen Regel darstellt.

6.1. Attribution

Die Attribution eines sicherheitspolitisch relevanten Cybervorfalls bezieht sich auf die Identifikation der Täterschaft und beschreibt einen ganzheitlichen interdisziplinären Prozess, der die Analyse technischer und rechtlicher Eigenschaften eines Cybervorfalls umfasst, den geopolitischen Kontext berücksichtigt und das gesamte nachrichtendienstliche Spektrum zur Informationsbeschaffung nutzt. Gestützt darauf kann ein Staat eine bestimmte Cyberoperation

---

relevant provisions of the United Nations Charter), to an international armed conflict, whatever type of weapons might be used." Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para 89.

15 Art. 2 und 3 Abkommen betreffend die Rechte und Pflichten der neutralen Mächte und Personen im Falle eines Landkriegs (18. Oktober 1907), SR 0.515.21; Art. 2 und 5 Abkommen betreffend die Rechte und Pflichten der neutralen Mächte und Personen im Falle eines Seekriegs (18. Oktober 1907), SR 0.515.22.

16 Art. 1 Abkommen betreffend die Rechte und Pflichten der neutralen Mächte und Personen im Falle eines Landkriegs (18. Oktober 1907), SR 0.515.21.

17 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

öffentlich oder nicht öffentlich einem anderen Staat oder privaten Akteur zurechnen und weitere politische Massnahmen beschliessen.

Die rechtliche Attribution ist ein Teil der oben beschriebenen Analyse. Sie betrifft die Frage, ob ein Cybervorfall völkerrechtlich einem anderen Staat zugerechnet werden kann und ob dieser Staat gemäss den Regeln zur Staatenverantwortlichkeit völkerrechtlich zur Verantwortung gezogen werden könnte bzw. wie der betroffene Staat im Rahmen des Völkerrechts darauf reagieren darf (sog. Gegenmassnahmen siehe Ziff. 6.2). Das Handeln staatlicher Organe und von Personen, die inhärent staatliche Funktionen ausüben, sind dem Staat rechtlich immer zurechenbar.[18] Führen nichtstaatliche Akteure einen Cybervorfall durch, können solche Handlungen einem Staat nur unter bestimmten Voraussetzungen zugerechnet werden. Die anwendbaren Kriterien der Staatenverantwortlichkeit verlangen in einem solchen Fall, dass nichtstaatliche Akteure im Auftrag eines Staates oder unter der Leitung oder Kontrolle staatlicher Organe handeln.[19] Trifft dies zu, ist ihr Verhalten als Handlung des Staates zu werten und wird dem Staat zugerechnet. Der betroffene Staat darf Gegenmassnahmen ergreifen (siehe Ziff. 6.2). Fehlt die notwendige zwischenstaatliche Dimension, so sind Gegenmassnahmen gegen einen anderen Staat grundsätzlich völkerrechtlich unzulässig.

Entscheide im Zusammenhang mit der Attribution liegen im Ermessen des betroffenen Staates. Es gibt keine völkerrechtliche Verpflichtung, Informationen offenzulegen, die zu entsprechenden staatlichen Entscheiden geführt haben. Vorwürfe der Organisation und Durchführung unrechtmässiger Handlungen, die gegen Staaten erhoben werden, sollten aber begründet werden.[20]

6.2. Gegenmassnahmen

Staaten dürfen auf unerwünschte Handlungen anderer Staaten im Cyberraum je nach Sachverhalt auf unterschiedliche Weise reagieren.

Mit Retorsion dürfen Staaten immer auf unerwünschte Handlungen anderer Staaten im Cyberraum reagieren, unabhängig davon, ob es sich um eine Völkerrechtsverletzung handelt oder nicht. Unter Retorsion werden unfreundliche, aber völkerrechtskonforme Massnahmen in Reaktion auf eine vorangehende unerwünschte staatliche Handlung verstanden. Herkömmliche Beispiele dafür sind der Nichtabschluss eines für die Gegenseite interessanten Handelsvertrages, der Rückruf eines Botschafters oder, als ultima ratio, der Abbruch diplomatischer Beziehungen.

Bei Vorliegen einer völkerrechtswidrigen Handlung und der rechtlichen Attribution dürfen Staaten unter Einhaltung der entsprechenden Regeln zur Staatenverantwortlichkeit auch Gegenmassnahmen im Sinne von Repressalien ergreifen.[21] Repressalien sind eigentlich völkerrechtswidrige Massnahmen, die als Reaktion auf einen vorangehenden Völkerrechtsbruch gerechtfertigt sind. Gewisse sanktionsfeste Normen dürfen allerdings durch eine Gegenmassnahme nicht gebrochen werden. Hierzu gehören das Gewaltverbot, grundlegende Menschenrechte, die meisten Normen des humanitären Völkerrechts, Normen mit *ius cogens*-Charakter, sowie der Grundsatz der Unverletzlichkeit der diplomatischen und

---

18 Art. 4, 5 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.
19 Art. 8 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.
20 UN GGE Bericht 2015, 28 f).
21 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001. Soweit nicht völkerrechtlich verboten, sind Repressalien an strenge Bedingungen geknüpft.

konsularischen Einrichtungen.[22] Ausgeschlossen ist daher die Anwendung militärischer Gewalt, d.h. von Massnahmen, die zu Verlust von Leib und Leben führen.

Gegenmassnahmen müssen immer darauf abzielen, mittels Zufügung von (Rechts-) Nachteilen den betreffenden Staat zur Einstellung seines völkerrechtswidrigen Verhaltens und/oder zu einer Wiedergutmachung zu bewegen. Sie können grundsätzlich erst ergriffen werden, wenn der verantwortliche Staat vorgängig zur Einstellung des Völkerrechtsbruchs aufgefordert und die Gegenmassnahme angekündigt wurde. Im Kontext von Cyberoperationen kann ausnahmsweise von dieser Vorgabe abgewichen werden, wenn eine unmittelbare Reaktion zwingend notwendig ist, um die Rechte des betroffenen Staates durchzusetzen und weiteren Schaden zu vermeiden. Gegenmassnahmen sind in jedem Fall nur zulässig, wenn sie verhältnismässig sind.

Gegenmassnahmen als Reaktion auf einen Cybervorfall müssen nicht unbedingt im Cyberbereich erfolgen. Nach den Regeln der Staatenverantwortlichkeit sind auch anderweitige Gegenmassnahmen zulässig, mittels welchen die Einhaltung der völkerrechtlichen Plichten durch den verantwortlichen Staat erreicht wird. Bei Gegenmassnahmen, die sich im Cyberbereich selbst abspielen, ist es nicht notwendig, dass sie sich direkt gegen das Computersystem, von welchem der Vorfall ausgeht, richten. Es sind auch andere Cybermassnahmen möglich, solange diese das Ziel verfolgen, den anderen Staat zur Einstellung des ursprünglichen völkerrechtswidrigen Verhaltens zu bringen. So kann es abhängig von den konkreten Umständen völkerrechtlich zulässig sein, dass das Urheber-Computersystem im Ausland mittels Cybermassnahmen gestoppt wird; ebenso kann es im Einzelfall zulässig sein, dass Computersysteme im Ausland beeinträchtigt werden, die aber selbst nicht am Ursprung des Cybervorfalls standen.

Neben Gegenmassnahmen sehen die Regeln zur Staatenverantwortlichkeit auch besondere Umstände vor, die die Unrechtmässigkeit von staatlichem Handeln ausschliessen können. Diese können gegeben sein, wenn die Nicht-Einhaltung einer völkerrechtlichen Pflicht für einen Staat die einzige Möglichkeit darstellt, essentielle Interessen vor einer unmittelbaren und schweren Gefahr zu schützen. Im eng vorgegebenen Rahmen der in den Regeln zur Staatenverantwortlichkeit vorgesehenen Ausnahmen dürfen Staaten auch im Kontext von Cyberoperationen von völkerrechtlichen Pflichten abweichen.[23]

6.3. Due Diligence Sorgfaltspflichten

Due Diligence ist ein Prinzip, das sich über einen langen Zeitraum hinweg entwickelt hat und heute nach Ansicht der Schweiz Teil des Völkergewohnheitsrechts ist und auch im Cyberraum Anwendung findet. Der IGH umschreibt den allgemeinen Due Diligence Verhaltensstandard als «*every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States*». Demnach müssen Staaten diese Sorgfaltspflichten beachten betreffend Handlungen, die innerhalb ihres Hoheitsgebiets stattfinden und welche die Rechte anderer Staaten verletzen.[24] Due Diligence spiegelt fundamentale Prinzipien des Völkerrechts wieder (darunter staatliche Souveränität, Gleichheit, territoriale Integrität und Nichteinmischung).

---

22 Art. 50 ILC Draft Articles on State Responsibility.

23 Kapitel V, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

24 Corfu Channel case, I.C. J. Reports 1949, para 44. Due Diligence ist einerseits ein allgemeines völkerrechtliches Prinzip, das völkergewohnheitsrechtlich anerkannt ist und andererseits in internationalen Abkommen in verschiedenen Rechtsbereichen verankert und konkretisiert bzw. weiterentwickelt worden (z.B. Umweltrecht, Menschenrechte, humanitäres Völkerrecht, internationales Gesundheitsrecht).

Dieses Prinzip gilt auch im Cyberraum. Folglich muss ein Staat, der von solchen Vorgängen Kenntnis hat oder haben müsste, alle ihm vernünftigerweise möglichen, geeigneten Massnahmen treffen, um Cybervorfälle, die die Rechte anderer Staaten verletzen, zu beenden oder deren Risiken zu minimieren. Due Diligence ist ein variabler Standard und hängt von den Kapazitäten und Möglichkeiten eines Staates, sowie von den besonderen Umständen des jeweiligen Falles ab. Sie verpflichtet den Territorialstaat, alle ihm vernünftigerweise zur Verfügung stehenden Mittel einzusetzen, um zu verhindern, dass einem anderen Staat durch Aktivitäten, die in seinem Hoheitsgebiet oder in einem Gebiet unter seiner tatsächlichen Kontrolle stattfinden, ernsthafter Schaden zugefügt wird. Die Sorgfaltspflicht ist somit eine Verhaltens- und keine Ergebnispflicht. Der verantwortliche Staat ist bei Vorliegen der genannten Voraussetzungen völkerrechtlich verpflichtet, die Schutzlücken umgehend zu schliessen und bei der Abwehr und Rückverfolgung des Vorfalls behilflich zu sein.

Due Diligence gilt insbesondere in Konstellationen, in denen Handlungen Privater die Rechte anderer Staaten verletzen (z.B. Hackergruppen), die dem Staat gemäss den Regeln der Attribution nicht oder nicht eindeutig zugerechnet werden können (siehe Ziff. 6.1). Erfüllt der verantwortliche Staat die verlangten Sorgfaltspflichten bei Vorliegen der genannten, erforderlichen Kriterien nicht, kann der verletzte Staat unter Beachtung der Regeln zur Staatenverantwortlichkeit Gegenmassnahmen ergreifen, um den verantwortlichen Staat zu veranlassen, seine Verpflichtungen zu erfüllen. Bei diesen Gegenmassnahmen handelt es sich um die oben dargelegten Optionen sowohl ausserhalb wie innerhalb des Cyberbereichs. Der verantwortliche Staat kann zudem dazu angehalten werden, Wiedergutmachung zu leisten.[25]

7. Menschenrechte

Die Menschenrechte sind ein zentraler Grundpfeiler des Völkerrechts. Sie sind in verschiedenen völkerrechtlichen Verträgen garantiert, unter anderem im UNO Pakt über bürgerliche und zivile Rechte (UNO-Pakt II) sowie in der Europäischen Konvention für Menschenrechte (EMRK). Die grundlegenden Menschenrechte sind auch Teil des Völkergewohnheitsrechts und stellen teilweise *ius cogens* dar. Den Menschenrechten werden heute mehrere Verpflichtungsdimensionen beigemessen: Neben dem abwehrrechtlichen Schutz vor staatlichen Eingriffen (Achtungspflichten bzw. Abwehrrechte; «obligations to respect») gewährleisten sie staatlichen Schutz vor Eingriffen durch Dritte (Schutzpflichten; „obligations to protect“) und verpflichten die Staaten, die Ausübung eines Rechts durch positive Massnahmen überhaupt erst zu ermöglichen (Gewährleistungspflichten; „obligations to fulfill“).

Die Menschenrechte gelten auch im digitalen Raum und stellen einen zentralen Pfeiler des internationalen Regelwerks der Digitalisierung dar. Individuen haben bei allen digitalen Aktivitäten deshalb die gleichen Rechte, wie sie dies im physischen Raum auch haben. Dies gilt auch bei sicherheitspolitischen Aktivitäten von Staaten, die sich im Cyberraum und damit einem Teilbereich des digitalen Raums abspielen: Wenn Staaten im Cyberraum operieren, sind sie an ihre Menschenrechtsverpflichtungen genauso gebunden, wie wenn sie im physischen Raum operieren. Dies gilt auch dann, wenn diese Cyberoperationen extraterritorial erfolgen, soweit die Staaten dabei Hoheitsgewalt ausüben. Kommt es zu Verletzungen der Menschenrechte durch cyberbezogene Aktivitäten, so stehen den betroffenen Einzelpersonen grundsätzlich die anwendbaren innerstaatlichen und völkervertraglich vorgesehenen Durchsetzungsmechanismen genauso zu Verfügung, wie

[25] Art. 31, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

wenn die Verletzung im physischen Raum erfolgen würde. Die Praxis der internationalen Kontrollorgane und Spruchkörper kann sich dabei in Bezug auf die Reichweite und Anwendbarkeit der Menschenrechte weiterentwickeln.

Eine Reihe spezifischer Menschenrechte können bei cyberbezogenen Aktivitäten besonders betroffen sein: Beispielsweise könnte das Recht eines Individuums auf Zugang zu Informationen, auf Privatsphäre oder auf freie Meinungsäusserung aufgrund von Cyberoperationen oder weiterer cyberbezogener Massnahmen beschränkt werden.

Staaten müssen Einschränkungen dieser und weiterer Menschenrechte im Cyberraum auf Basis der gleichen Regeln rechtfertigen können, wie dies im physischen Raum der Fall ist. Grundsätzlich erfordert ein Eingriff eine ausreichende gesetzliche Grundlage und der Staat muss im Rahmen einer Interessenabwägung darlegen, dass der Eingriff geeignet, erforderlich und zumutbar ist, um ein legitimes Ziel zu erreichen.

Während der Grundsatz, wonach die Menschenrechte auch im Cyberraum gelten, aus Sicht der Schweiz klar ist, können sich in Einzelfällen der Anwendung neue Fragen stellen. Wird beispielsweise mit cyberbezogenen Aktivitäten der Zugang zu sozialen Medien blockiert, so kann mit Blick auf das Recht auf freie Meinungsäusserung Klärungsbedarf bestehen, ab wann ein Eingriff in das geschützte Rechtsgut erfolgt, oder ob das Recht auch mittels alternativer Kommunikationsinstrumente wahrgenommen werden kann und inwieweit auch private Akteure durch Menschenrechte gebunden sind. Hier bedarf es in den zuständigen Foren für Fragen der Menschenrechte weitere Arbeiten, um die Verwirklichung der Menschenrechte im Cyberraum sicherzustellen.

II. Humanitäres Völkerrecht

Aus Sicht der Schweiz findet das Völkerrecht im Cyberraum Anwendung, was während bewaffneten Konflikten ebenfalls für das humanitäre Völkerrecht (HVR) gilt. Die Einhaltung, Stärkung und Förderung des HVR zählt zu den aussenpolitischen Prioritäten der Schweiz, denn sie zeichnet sich durch ihre Neutralität, ihre humanitäre Tradition und ihren Status als Depositarstaat der Genfer Konventionen aus. In der vorliegenden nationalen Position geht die Schweiz deshalb vertieft auf Fragen des HVR ein.

1. Anwendbarkeit des HVR

Das HVR findet Anwendung, sobald ein internationaler oder nicht internationaler bewaffneter Konflikt faktisch vorliegt. Das HVR gilt in jedem bewaffneten Konflikt und für alle Konfliktparteien. Es befasst sich mit den Realitäten des Krieges, unabhängig von den Gründen oder der Rechtmässigkeit der Gewaltanwendung. Es gibt keine Antwort auf die Frage der Rechtmässigkeit eines Kriegs und legitimiert diese zwischenstaatliche Gewaltanwendungen nicht. [26] Es hat zum Ziel, die Kriegsführung zu regeln und die Opfer von bewaffneten Konflikten zu schützen, indem es vor allem den Einsatz von Mitteln und Methoden der Kriegsführung einschränkt. Der IGH hat festgehalten, dass die etablierten Prinzipien und Regeln des HVR

[26] Jede Anwendung von Gewalt zwischen Staaten ist durch die UNO-Charta und das relevante Völkergewohnheitsrecht geregelt (siehe oben, Ziff. I.4.).

für alle Formen der Kriegsführung und für alle Arten von Waffen gelten, diejenigen aus der Vergangenheit, der Gegenwart und der Zukunft.[27]

Das gilt für den Cyberraum wie es auch für die herkömmlichen und für die neuen Operationsräume gilt (etwa den Weltraum, die Luft, den Boden, den maritimen Raum, den elektromagnetischen Raum, und den Informationsraum). Somit ist das HVR der wichtigste völkerrechtliche Rechtsbereich für die Regelung von Cyberoperationen mit Bezug zu bewaffneten Konflikten. Eine effektive Umsetzung des HVR trägt zur Gewährleistung der internationalen Sicherheit bei. Das bestehende HVR, insbesondere seine Grundprinzipien, setzt der Durchführung von Cyberoperationen in bewaffneten Konflikten wichtige Grenzen.

2. Grundlegende Bestimmungen des HVR zur Regelung der Kriegsführung

2.1. Grundsatz betreffend Mittel und Methoden der Kriegsführung

Das HVR verbietet oder beschränkt Mittel (Waffen) und Methoden der Kriegsführung einerseits durch allgemeine Prinzipien, die das Verhalten regeln oder bestimmte Wirkungen verbieten. Es tut dies andererseits auch durch spezifische Regeln, die sich auf bestimmte Mittel oder Methoden der Kriegsführung beziehen. Bei Waffen muss zwischen der Rechtmässigkeit eines bestimmten Waffentyps an sich (Waffenrecht) und der Rechtmässigkeit der Art und Weise, in der die Waffe eingesetzt wird (*targeting law*), unterschieden werden. Die inhärenten Eigenschaften bestimmter Waffenkategorien können dazu führen, dass ihre Verwendung - unter gewissen oder allen Umständen - per se rechtswidrig ist. Die Zulässigkeit aller anderen Waffen hängt davon ab, ob ihr Einsatz in Übereinstimmung mit dem HVR erfolgt.

Das gilt auch für den Cyberraum. Tatsächlich müssen die Entwicklung und der Einsatz neuer Mittel und Methoden der Kriegsführung im Einklang mit dem geltenden Völkerrecht, insbesondere mit dem HVR, stehen. Das gilt auch dann, wenn eine Waffe nicht von einer spezifischen Norm erfasst wird und sich die Vertragsbestimmungen zur Regelung der Kriegsführung nicht ausdrücklich auf neue Technologien beziehen. Die gewohnheitsrechtlichen Regeln des HVR finden auf alle Mittel und Methoden der Kriegsführung, d.h. auch im Cyberraum, gleichermassen Anwendung. So ist es ein seit langem bestehender Grundsatz, dass die am Konflikt beteiligten Parteien kein unbeschränktes Recht in der Wahl der Mittel und Methoden der Kriegsführung haben.

2.2. Rechtmässigkeit eines bestimmten Waffentyps an sich

Gemäss HVR ist jedes Mittel oder jede Methode der Kriegsführung, die eines oder mehrere der folgenden Merkmale aufweist, per se rechtswidrig:

Das Mittel oder die Methode der Kriegsführung:

(1) ist dazu geeignet, überflüssige Verletzungen oder unnötige Leiden zu verursachen;
(2) wirkt unterschiedslos, weil es nicht gegen ein bestimmtes militärisches Ziel gerichtet werden kann oder weil seine Auswirkungen nicht entsprechend den Vorschriften des HVR begrenzt werden können;

---

[27] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 86; "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future".

(3) ist dazu bestimmt, oder es kann von ihm erwartet werden, ausgedehnte, langanhaltende und schwere Schäden der natürlichen Umwelt zu verursachen; *oder*
(4) ist vertrags- oder gewohnheitsrechtlich ausdrücklich verboten.

Das gilt auch im Cyberraum und somit für Cybermittel und -methoden der Kriegsführung.

2.3. Rechtmässigkeit der Art und Weise, in der die Waffe eingesetzt wird

Im Hinblick auf den rechtmässigen Einsatz von Mittel und Methoden der Kriegsführung müssen die Regeln und Grundprinzipien der Kriegsführung eingehalten werden. Dazu müssen die Kriegführenden insbesondere die Prinzipien der Unterscheidung, der Verhältnismässigkeit und der Vorsichtsmassnahmen beachten, nämlich:

(1) unterscheiden zwischen militärischen Zielen einerseits und Zivilisten oder zivilen Objekten andererseits und im Zweifelsfall einen zivilen Status vermuten;
(2) beurteilen, ob der zu erwartende Schaden für die Zivilbevölkerung oder zivile Objekte in keinem Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil stünde;
(3) alle praktisch möglichen Vorsichtsmassnahmen treffen, um geschützte Personen und Objekte von den Folgen der Kriegshandlungen zu verschonen.

Das gilt auch im Cyberraum für den Einsatz von Cybermitteln und –methoden der Kriegsführung. Diese Prinzipien regeln insbesondere Cyber-Operationen, die einem Angriff im Sinne des HVR gleichkommen, d.h. sowohl eine offensive als auch eine defensive Gewaltanwendung gegen den Gegner. Was genau in einem bewaffneten Konflikt als «Cyberangriff» gilt, bleibt zu klären. Erfasst sind zumindest Cyber-Operationen, von denen erwartet werden kann, dass sie direkt oder indirekt die Verletzung oder den Tod von Personen oder die physische Beschädigung oder Zerstörung von Objekten verursachen. Eine Herausforderung bleibt die Frage, wie genau Daten geschützt sind, wenn keine physischen Schäden entstehen. In der Praxis sollte ein verantwortungsbewusster Akteur grundsätzlich die möglichen Auswirkungen seines Verhaltens und Schäden abschätzen können. Da dies unter anderem stark von den bei der Entscheidung verfügbaren Informationen abhängt, kommt der Verpflichtung, alle praktisch möglichen Vorsichtsmassnahmen zu treffen, um Zivilpersonen und zivile Objekte zu verschonen, beim Einsatz von Cybermitteln und -methoden der Kriegsführung eine besonders wichtige Rolle zu.

3. Andere Bestimmungen des HVR

Die Pflicht zur vollständigen Einhaltung des HVR beschränkt sich nicht auf die Regeln und Prinzipien der Kriegsführung. Weitere spezifische Regeln des HVR müssen respektiert werden, auch bei militärischen Operationen, die keine «Angriffe» darstellen. So stehen etwa bestimmte Kategorien von Personen und von Objekten unter besonderem Schutz. Medizinisches, religiöses oder humanitäres Personal und diesem Zweck dienende Objekte müssen beispielsweise unter allen Umständen geschont und geschützt werden.

Dies gilt ebenfalls im Cyberraum. Bei Cyber-Operationen, welche einen Bezug zu solchen besonders geschützten Personen und Objekten oder zu anderen vom HVR-geregelten Sachverhalten haben, müssen alle relevanten spezifischen Regeln berücksichtigt werden.

4. Sicherstellung der Einhaltung des HVR

Staaten und die am Konflikt beteiligten Parteien haben eine übergeordnete Verpflichtung, das HVR unter allen Umständen einzuhalten und seine Einhaltung durchzusetzen. Es ist unbestritten, dass Vorbereitungsmassnahmen getroffen werden müssen, um die Umsetzung des HVR zu ermöglichen, und dass diese Umsetzung überwacht werden muss. Aufgrund dieser Verpflichtung müssen die Staaten und die am Konflikt beteiligten Parteien unter anderem Massnahmen ergreifen, um sicherzustellen, dass die Entwicklung und der Einsatz von Mitteln und Methoden der Kriegsführung in vollem Einklang mit dem HVR stehen und Ergebnisse verhindern, die rechtswidrig wären.

Das gilt auch für den Cyberraum und Cybermittel und -methoden der Kriegsführung. Wie bei jeder anderen Waffe, Mittel oder Methode der Kriegsführung haben die Staaten die positive Verpflichtung, bei ihrer Prüfung, Entwicklung, Beschaffung oder Einführung festzustellen, ob ihre Verwendung stets oder unter bestimmten Umständen gegen das bestehende Völkerrecht verstossen würde. In dieser Hinsicht stellt die Pflicht zur Durchführung rechtlicher Überprüfungen von neuen Waffen, wie sie in Artikel 36 des 1. Zusatzprotokolls zu den Genfer Abkommen festgelegt ist[28], ein wichtiges Element dar, um die Entwicklung und den Einsatz neuer Cyberwaffen, die insbesondere die oben aufgeführten Verpflichtungen nicht erfüllen würden, zu verhindern oder einzuschränken.

[28] Zusatzprotokoll zu den Genfer Abkommen vom 12. August 1949 über den Schutz der Opfer internationaler bewaffneter Konflikte (Protokoll I), SR 0.518.521.