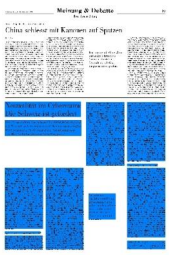
Datum: 30.12.2020

Neue Zürcher Zeitung



Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 91'624
Erscheinungsweise: 6x wöchentlich

Seite: 19
Fläche: 70'520 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 79361543
Ausschnitt Seite: 1/3

Neutralität im Cyberraum: Die Schweiz ist gefordert

Viele Staaten rüsten ihre militärischen IT-Kapazitäten massiv auf. Nun will auch die Schweiz ein Cyberkommando schaffen. Was bedeutet dies für die Neutralität? ***Gastkommentar von Martin Dahinden und Sara Pangrazzi***

Die Bedeutung von Cyberangriffen nimmt rasant zu: Das prominente Schadprogramm WannaCry beispielsweise hat seit seiner Entdeckung im Mai 2017 innert kurzer Zeit weltweit mehr als 200 000 Computer infiziert und international für Schlagzeilen gesorgt. Betroffen waren Rechner des russischen Innenministeriums und zahlreicher Spitäler in Grossbritannien, der Autohersteller Renault-Nissan oder auch die Deutsche Bahn. Das Programm nutzte eine Sicherheitslücke im weltweit breit genutzten Windows-Betriebssystem aus und führte zu Schäden in Milliardenhöhe. Auch die Schweizer Bundesverwaltung hat regelmässig mit digitalen Angriffen zu kämpfen: Im September 2017 etwa wurden laut einer Medienmitteilung Cyberangriffe auf das Verteidigungsdepartement (VBS) entdeckt, und im Januar 2016 haben ebensolche beim Rüstungskonzern Ruag zur Entwendung von Daten im Umfang von mehr als 20 Gigabyte geführt. Die technische Rückverfolgung der jeweiligen Urheber hält Informatiker bis heute auf Trab.

Um diese Risiken zu bewältigen, rüsten Staaten ihre militärischen IT-Kapazitäten auf. Auch die Schweiz baut ihre digitalen Kapazitäten aus und plant den Aufbau eines Cyberkommandos. Weil bezüglich der Anwendung internationaler Normen auf Cyberangriffe allerdings noch viele Unklarheiten bestehen, gibt es neben den technischen auch erhebliche rechtliche und politische Herausforderungen.

Cyberangriffe als bewaffnete Angriffe?

Mit dem Cyberkommando möchte der Bundesrat die digitale Verteidigung der Schweizer Armee stärken. Die am 1. März 2019 in Kraft getretene Verordnung über die militärische Cyberabwehr (MCAV) regelt Aktionen im Cyberraum zum Eigenschutz und zur «Selbstverteidigung» der Schweizer Armee gegen Cyberangriffe. Doch was wird unter Selbstverteidigung gegen Cyberangriffe verstanden? Massnahmen der Selbstverteidigung gegen andere Staaten müssen nicht nur die Voraussetzungen des nationalen Rechts erfüllen, sondern immer auch völkerrechtlich zulässig sein – insbesondere wenn sie über den Schutz hinausgehen und offensive Abwehrmassnahmen beinhalten.

Bereits 2013 und 2015 haben von der Uno eingesetzte Expertengruppen festgehalten, dass das traditionelle Völkerrecht und somit die Uno-Charta auf den Cyberraum anwendbar sei. Allerdings besteht bis heute Uneinigkeit darüber, wie diese Normen konkret angewendet werden sollen. Die Komplexität und Neuartigkeit des Themas sowie die divergierenden politischen Interessen erschweren eine Konsensfindung zwischen den Staaten massiv. Eine Schlüsselfrage ist, ob und ab welcher Intensität Cyberangriffe gemäss Art. 51 der Uno-Charta bewaffnete Angriffe darstellen, dadurch die «Kriegsschwelle» überschreiten und offensive Selbstverteidigungshandlungen legitimieren, die mit militärischen Mitteln auch ausserhalb des Cyberraums erfolgen können. Dieses Recht auf Selbstverteidigung stellt eine Ausnahme vom grundsätzlich global geltenden Verbot der Gewalt zwischen Staaten dar.

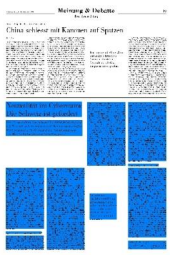
Die meisten Staaten bejahen, dass Cyberangriffe die erwähnte Schwelle erreichen können, wenn sie dieselben Effekte haben wie herkömmliche bewaffnete Angriffe. Uneinigkeit besteht allerdings darüber, welche Effekte im digitalen Kontext genau darunterfallen. Gemäss dem traditionellen Völkerrechtsverständnis müssen bewaffnete Angriffe physische Zerstörung und/oder Todesopfer nach sich ziehen. Der Uno-Sicherheitsrat hat ökonomische oder politische Schäden für die Einstufung als bewaffneter Angriff noch nie als ausreichend beurteilt.

Datum: 30.12.2020

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 91'624
Erscheinungsweise: 6x wöchentlich



Seite: 19
Fläche: 70'520 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 79361543
Ausschnitt Seite: 2/3

Schwierigkeiten beim Aufeinandertreffen von traditionellen Völkerrechtsnormen und Cyberangriffen bereitet zunächst, dass digitale Angriffe nicht im herkömmlichen Sinne «bewaffnet» sind. Grundsätzlich bewirken sie nämlich Funktionsstörungen an Computersystemen, womit sie primär nicht physischer Natur sind. Die durch Datenverluste, Informationsverzerrungen oder Softwaremanipulationen mittelbar ausgelösten Schädigungen sind überwiegend ebenfalls nicht physisch und generell schwer bezifferbar. Grossflächige und für einen bewaffneten Angriff überhaupt infrage kommende Zerstörungen durch Cyberangriffe gab es bis dato zudem nur sehr wenige. Cyberangriffe erfüllen daher nur selten – wenn überhaupt – die Voraussetzungen von Art. 51 der Uno-Charta. Man befindet sich regelmässig ausserhalb des Anwendungsbereichs der Selbstverteidigung, wenn Cyberangriffe keine physische Zerstörung zur Folge haben und/oder Todesopfer fordern.

Cyberangriffe sind technisch schwer zurückzuverfolgen und können rechtlich bisweilen nicht eindeutig einem Staat zugerechnet werden. Dies wird dadurch erschwert, dass sie häufig Teil einer hybriden Kriegsführung sind, die neben staatlichen auch nichtstaatliche Akteure einschliesst. Bei Cyberangriffen sind oft mehrere Staatsterritorien gleichzeitig betroffen. Meist ist nicht einmal ganz klar, ob ein gezielter Angriff oder ein Kollateralschaden eines Angriffs vorliegt, da sich Computerwürmer grundsätzlich automatisch auf viele Systeme weiterverbreiten. Angreifer nutzen zudem oft die Infrastruktur (vieler) unbeteiligter Dritter als Brückenkopf, um anonym zu bleiben. Bei der Eruierung des tatsächlichen Urhebers von Cyberangriffen handelt es sich wegen der schwierigen technischen und rechtlichen Zurechnung somit oft – wenn nicht überwiegend – um Zweifelsfälle. Gegenschläge können leicht unbeteiligte Drittstaaten treffen. Deshalb scheint grosse Zurückhaltung geboten.

> Massnahmen der Selbstverteidigung müssen immer auch völkerrechtlich zulässig sein – insbesondere wenn sie offensive Abwehrmassnahmen beinhalten.

Im Zusammenhang mit der schweizerischen Neutralität gibt es zusätzliche Herausforderungen. Neben generellen Völkerrechtsnormen sind auch Neutralitätsverpflichtungen zu beachten. Die Neutralität verpflichtet die Schweiz, nicht an Kriegen teilzunehmen, Konfliktparteien gleich zu behandeln und den Kriegsparteien ihr Staatsgebiet nicht zur Verfügung zu stellen. Was heisst das im Cyberkontext?

Wegen der weltweit zunehmenden Vernetzung von Netzwerkinfrastrukturen sowie der globalen Verteilung digitaler Programme durchqueren Cyberangriffe von Konfliktparteien regelmässig neutrale private und/oder öffentliche Infrastrukturen. Das wirft heikle Fragen zu völkerrechtlichen Sorgfaltspflichten (Due Diligence) eines neutralen Staates auf. Ein Staat ist für völkerrechtlich relevante Verletzungen eines anderen Staates, die von seinem Territorium ausgehen, grundsätzlich verantwortlich, wenn er Kenntnis davon hat und die Möglichkeit, sie zu unterbinden oder zu beenden. Wie weit diese Due-Diligence-Normen im Cyberraum anwendbar sind, ist umstritten.

Glaubwürdig bleiben – aber wie?

Der Neutralitätsstatus hat zudem Vorwirkungen in Friedenszeiten. Ein dauernd neutraler Staat wie die Schweiz darf insbesondere keine Bindungen eingehen, die im Kriegsfall seine Neutralität gefährden oder unglaubwürdig machen. Unklar ist, wie diese Verpflichtungen im Cyberbereich anzuwenden sind und welche Möglichkeiten und Grenzen damit für die internationale Zusammenarbeit bestehen.

Eine besondere Herausforderung ist vor dem Hintergrund der Due-Diligence-Verpflichtung auch die Kontrolle von digitalen (Dual-Use-)Technologien. Unter anderem fragt sich, welche Kontrollmassnahmen erforderlich sind, damit die Schweiz ihren Neutralitätsverpflichtungen und anderen aussenpolitischen Zielen nachkommen kann, wenn sie solche Technologien herstellt oder weitergibt, und wieweit sie verantwortlich ist, wenn diese Technologien völkerrechtswidrig eingesetzt werden.

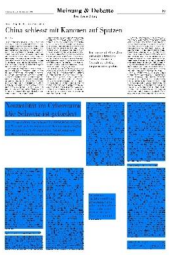
Als neutraler Kleinstaat hat die Schweiz ein Interesse an der Klärung der Anwendbarkeit völkerrechtlicher Normen bei Cyberangriffen sowie an einer wirksamen Rolle der Uno als Organisation kollektiver Sicherheit. Dies betrifft angesichts des Aufbaus eines Cyberkommandos insbesondere die Klärung des völkerrechtlichen Selbstverteidigungsrechts bei solchen Angriffen. Allerdings werden sie neutralitätsbezogene Fragen nicht lösen. Damit sich die Schweiz als neutraler Staat aussenpolitisch glaubwürdig positionieren kann, muss sie sich

Datum: 30.12.2020

Neue Zürcher Zeitung

Neue Zürcher Zeitung
8021 Zürich
044/ 258 11 11
https://www.nzz.ch/

Medienart: Print
Medientyp: Tages- und Wochenpresse
Auflage: 91'624
Erscheinungsweise: 6x wöchentlich



Seite: 19
Fläche: 70'520 mm²

Auftrag: 3007101
Themen-Nr.: 999.222

Referenz: 79361543
Ausschnitt Seite: 3/3

verstärkt um die neutralitätsbezogenen Aspekte der Cybersicherheitspolitik bemühen. Das Vorhaben der Schweiz, digitale Technologien mit einem Cyberkommando aufzurüsten, unterstreicht diese Dringlichkeit.

Martin Dahinden war Schweizer Botschafter in den USA, ist Mitglied des Stiftungsrates des Think-Tanks ICT4Peace und lehrt Sicherheitspolitik an der Universität Zürich; **Sara Pangrazzi** forscht am Institut für Völkerrecht an der Universität Zürich im Bereich der Cybersicherheit.