ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Alternativen zum „Hackback“? Staatliche Cybersicherheitsangriffe aus Sicht des Völkerrechts

Tanya Gärtner (M. lur.)
Mit einem technischen Problemaufriss von Donika Mirdita

Kurzzusammenfassung des gleichnamigen Vortrags im Rahmen der Veranstaltungsreihe „Rechtsrahmen der Cybersicherheitsforschung“

veranstaltet von Dr. Annika Selzer und Prof. Dr. Indra Spiecker gen. Döhmann

Impressum

Layout und Satz
Luise Charlotte Klett

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

Hinweise

Dieser Beitrag wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen.

Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Staatliche Cybersicherheitsangriffe und das Völkerrecht

Ein technischer Problemaufriss von Donika Mirdita

Large scale cyberattacks are carried out either directly by or using commercially available tools from criminal hacking groups. Nowadays launching cyberattacks does not necessarily require setting up a vast network of infected machines of your own nor extraordinary technical skills, you can just purchase on the dark web computing time from existing attack infrastructure to launch cyberattacks. This infrastructure has already been created by large hacker groups and you can buy firepower for as little as 20 euros a month. This is a massive red flag for cyberdefense because it lowers the entry barrier to carry out cyberattacks by a large factor.

Passive cyberdefense such as detection, traffic filtering on the victim's end and forensics investigation after an attack are no longer scalable or efficient given the frequency, scale and potentially life-threatening consequences of cyberattacks on services and infrastructure.

ENISA (the EU agency for cybersecurity) listed state-sponsored threat actors as one of the main threat vectors in cybersecurity for 2022. While some cyberattacks are carried out purely for self-enrichment on the part of cybercriminlas, there are campaigns that have political agendas. In the past year alone there have been several cyberattacks on government infrastructure of EU and NATO countries, in many cases the post-attack forensics was able to establish government actors behind them.

Due to this intricate relationship between hackers and government, it inevitably follows that sometime resources between these entities can also overlap. It is important however that active cyberdefense should not provide casus belli for escalation and there are ways to avoid that. As a rule of thumb, governments do not take ownership or responsibility for what the hackers operating in their country do, but an uncontrolled unregulated reactive cyberdefense could potentially spill into damaging legitimate national infrastructure which could constitute an escalation. As a result, active cyberdefense while a much needed evolution of existing cybersecurity strategies, needs a technical and legal framework informed by all security shareholders in a democratic state: law enforcement, government, industry experts and cybersecurity researchers that inform the appropriate steps to counter an attack in order to maximize protection while minimizing any unwanted consequences on internet infrastructures at large.

Donika Mirdita is a cybersecurity researcher at ATHENE and PhD Candidate at the Technical University Darmstadt.

Alternativen zum „Hackback“? Staatliche Cybersicherheitsangriffe aus Sicht des Völkerrechts

§

Ein rechtlicher Kurzüberblick von Tanya Gärtner (M. iur.)

1. Was ist Völkerrecht?

“Völkerrecht” ist das Recht zwischen Völkerrechtssubjekten, die zwar nicht nur, aber vorrangig Staaten sind.[1] Das Völkerrecht legt Staaten Rechte und Pflichten auf, die ihren Umgang miteinander bestimmen.[2] Auch internationale Organisationen, wie die Vereinten Nationen, sind in gewissem Maße Völkerrechtssubjekte.[3] Lebensbereiche, in denen das Völkerrecht seine Wirkung entfaltet, sind unter anderem diplomatische Beziehungen, Friedenssicherung und bewaffnete Konflikte, Umwelt- und Klimaschutz, Luft- und Raumfahrt, internationale Wirtschaft und der Abbau von Handelshemmnissen sowie die aktuellen Entwicklungen der Informationstechnik. Das Völkerrecht hat sich über Jahrhunderte entwickelt und entwickelt sich immer noch – nicht zuletzt hinsichtlich der Regulierung des Cyberraumes.

Zu den grundlegenden Rechtsinstituten des Völkerrechts gehören insbesondere der Grundsatz der souveränen Gleichheit der Staaten, das Interventionsverbot und das Gewaltverbot.

2. Wesentliche Rechtsgrundsätze im Völkerrecht

Der Grundsatz der souveränen Gleichheit der Staaten beschreibt im völkerrechtlichen Kontext die rechtliche Gleichheit und ausschließliche Hoheitsgewalt auf dem eigenen Territorium aller Staaten.[4] Daran anknüpfend verbietet das Interventionsverbot die Einmischung in die eigenen Angelegenheiten eines Staates durch die Anwendung oder Androhung von Zwang.[5] Das Gewaltverbot ist in Art. 2 Nr. 4 der UN-Charta verankert und verpflichtet Staaten zum Verzicht auf Gewalt in ihren internationalen Beziehungen. Hierfür gibt es nur wenige Ausnahmen, zum Beispiel das Recht auf Selbstverteidigung gegen einen bewaffneten Angriff gemäß Art. 51 der UN-Charta, sowie Zwangsmaßnahmen des UN-Sicherheitsrates gemäß Kapitel VII der UN-Charta.

Aus dem Verstoß gegen eine völkerrechtliche Norm entsteht die Pflicht des rechtbrechenden Staates zur Wiederherstellung des völkerrechtsgemäßen Zustandes. Um dies zu erzwingen, ist es dem verletzten Staat möglich, bestimmte Gegenmaßnahmen zu ergreifen. Solche Gegenmaßnahmen sind die vorübergehende Nichterfüllung eigener völkerrechtlichen Pflichten durch den verletzten Staat gegenüber dem rechtbrechenden Staat. Diese Gegenmaßnahmen können jeglicher Art sein und zum Beispiel auch im Cyberraum stattfinden.[6]

3. Völkerrecht des Cyberraumes: Orientierungspunkte und Probleme

Auch wenn der Cyberraum keineswegs von Staatsgrenzen komplett unabhängig ist, stellt es das bisher raumbezogene Denken des Völkerrechts vor neuen Herausforderungen. Auch der Umstand, dass zunehmend Individuen, organisierte Gruppen und große Unternehmen über beträchtliche informationstechnische Fähigkeiten verfügen, ist dem Völkerrecht neu, das, wie eingangs erwähnt, vorrangig Staaten als Hauptakteure kennt.

Zur Beantwortung dieser und weiterer relevanten Fragen gab es in letzter Zeit unterschiedliche Versuche. Im Rahmen der Vereinten Nationen befassen sich zwei Gremien mit der Anwendung des Völkerrechts im Cyberraum, die United Nations Group of Governmental Experts (UN GGE) und die United Nations Open Ended Working Group (OWEG). Auch Unternehmen lieferten bereits Vorschläge für die Regulierung des Cyberraums, wie zum Beispiel Microsofts „Digital Geneva Convention“ oder die aus einer Kooperation zwischen mehreren Unternehmen hervorgegangene „Charter of Trust“. Darüber hinaus gibt es die Tallinn Manuals, die als wissenschaftliche Werke, auf Initiative des NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), das für Cyberhandlungen

---

[1] Arnauld: Völkerrecht, S. 1.

[2] Arnauld: Völkerrecht, S. 1.

[3] Arnauld: Völkerrecht, S. 21 ff.

[4] Delerue: Cyber Operations and International Law, S. 200 ff.

[5] IGH, Urt. II (Merits) v. 27.6.1986, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), ICJ Rep. 1986, 14, § 205.

[6] Schmitt: Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations, S. 111.

geltende Völkerrecht zusammenfassen. Inzwischen haben sich auch zahlreiche Staaten zu ihrer Einschätzung der Anwendung des Völkerrechts im Cyberraum geäußert.

4. Völkerrechtliche Erfassung der (internationalen) Cyberabwehr

Die Frage, genau welche Cyberhandlungen völkerrechtswidrig sind, ist allerdings noch nicht abschließend geklärt. Dies ist für betroffene Staaten deshalb besonders ungünstig, weil dadurch häufig auch die Rechtmäßigkeit bestimmter Cyberabwehrmaßnahmen unklar ist. Vor allem Maßnahmen der aktiven Cyberabwehr ähneln öfter den Methoden, die für Cyberangriffe genutzt werden, auch wenn sie einen völlig anderen Zweck – nämlich den Schutz unserer IT – verfolgen. An die Diskussion um die Rechtmäßigkeit der aktiven Cyberabwehr schließt sich auch die Frage nach der Bedeutung von sogenannten Hackbacks an, die zwar häufig mit Maßnahmen der aktiven Cyberabwehr verwechselt werden, jedoch eine völlig andere Ausrichtung haben (siehe unten).

Insbesondere reichte der bisherige internationale Konsens über die Anwendung des Völkerrechts im Cyberraum nicht für die Entstehung eines zwischenstaatlichen Vertrages, der diese Fragen regelt. Folglich muss die Rechtmäßigkeit einzelner Handlungen im Cyberraum noch an Völkergewohnheitsrecht oder an den völkerrechtlichen Rechtsgrundsätzen gemessen werden. In Betracht kommen insbesondere die oben erwähnten Rechtsinstitute des Gewaltverbots, des Interventionsverbots und der Grundsatz der staatlichen Souveränität.

5. Entwicklung einer Taxonomie der Cyberabwehr

Um im Rahmen des rechtlichen Diskurses auf den rechtssicheren Einsatz von Cyberabwehrmaßnahmen hinwirken zu können, bedarf es zunächst einer Schärfung des Verständnisses für die Begriffe der passiven und aktiven Cyberabwehr sowie der mit diesen Begriffen verbundenen Maßnahmen.

Unter Cyberabwehr versteht man technische Maßnahmen, die einen Cyberangriff verhindern oder stoppen, ohne hierbei einen digitalen Vergeltungsschlag zu verüben. Maßnahmen der passiven Cyberabwehr sind solche, die präventiv ergriffen werden, ohne dass ein konkreter Cyberangriff absehbar ist. Maßnahmen der aktiven Cyberabwehr sind hingegen solche, die reaktiv ergriffen werden, wenn ein konkreter Cyberangriff unmittelbar und absehbar bevorsteht oder bereits begonnen hat – dies umfasst keine digitalen Vergeltungsmaßnahmen. Hackbacks sind im Gegenzug „digitale Vergeltungsschläge", die nach Beendigung eines Cyberangriffs ergriffen werden und daher nicht mit aktiver Cyberabwehr gleichzusetzen sind.

Hackbacks und aktive Cyberabwehr unterscheiden sich somit insbesondere im Kontext ihrer Anwendung. Derweil Hackbacks nach Beendigung eines Cyberangriffs stattfinden und daher nicht direkt zum Schutz der eigenen IT-Infrastruktur beitragen können, ist es übergeordnetes Ziel der aktiven Cyberabwehr, im Rahmen einer Art „digitalen Notwehrlage", eine Risikobegrenzung für die angegriffene IT-Infrastruktur zu bewirken.

Die beiden Formen der Cyberabwehr lassen sich in Bezug auf ihren Wirkungsbereich weiter differenzieren: Maßnahmen, die der Abwehr von Cyberangriffen dienen, können entweder auf die zu verteidigenden IT-Infrastrukturen beschränkt sein und daher intern stattfinden, oder Auswirkungen haben, die über diese IT-Infrastrukturen hinausgehen und daher externer Natur sein bzw. (zusätzlich) extern wirken.[7]

Darüber hinaus können Maßnahmen mit (zusätzlich) externer Wirkung dahingehend unterschieden werden, ob die Maßnahmen intrusiv oder nicht intrusiv sind. Maßnahmen mit (zusätzlich) externer Wirkung sind intrusiv, wenn es aufgrund der Maßnahmen zu einem unbefugten Zugriff auf IT- Infrastrukturen oder die Beeinträchtigung ihrer Vertraulichkeit, Integrität oder Verfügbarkeit kommt bzw. der Versuch hierzu unternommen wird.[8] Nicht-intrusiv sind Maßnahmen mit (zusätzlich) externer Wirkung hingegen dann, wenn sie kein Eindringen in die IT-Infrastrukturen des Angreifers erfordern und auch nicht die Vertraulichkeit, Integrität oder Verfügbarkeit dieser beeinträchtigen.[9]

---

[7] So auch ähnlich Denning/Strawser, in Perkovich/Levite: Understanding Cyber Conflict, S. 198.

[8] National Institute of Standards and Technology, Intrusion, Glossary.

[9] Vgl. Shulman/Waidner, Aktive Cyberabwehr, S. 6 ff.; für das gesamte Unterkapitel siehe Gärtner/Selzer, Begriffsverwirrung verhindern: Was Maßnahmen Aktiver Cyberabwehr sind – und was nicht.

6. Fazit

Diese Einteilungen stellen einen Vorschlag dar, wie man Cyberabwehrmaßnahmen nach rechtlich relevanten Kriterien sortieren könnte. Welche dieser Arten von Cyberhandlungen sollten als Verstoß gegen das Völkerrecht gewertet werden? Welche dieser Kategorien sollten im Gegenzug als rechtmäßige Gegen- oder Abwehrmaßnahme verstanden werden?

Bis mehr Klarheit über die rechtliche Zulässigkeit der Erforschung und des Einsatzes der verschiedenen Formen von Cyberabwehrmaßnahmen geschaffen ist, sind die Erforschung und der Einsatz dieser Maßnahmen mit einem hohen Maß an Rechtsunsicherheit behaftet, was mittel- und langfristig zu einer Schwächung unserer IT und Gesellschaft führen könnte. Dementsprechend ist die rechtssichere Gestaltung des Einsatzes derartiger Maßnahmen von hohem gesellschaftlichem Interesse und bildet einen Schwerpunkt der rechtlichen Forschungsarbeiten des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE.

Oberste Priorität bei der Erforschung dieses Themenkomplexes haben dabei die Interessen der Gesellschaft, die einerseits von einer starken und sicheren IT-Landschaft, andererseits aber auch von Regeln für die Wissenschaft profitiert – denn Wissenschaft muss rechtssicher sein, darf aber nicht im rechtsfreien Raum erfolgen, sondern bedarf adäquater Regeln.

Eine saubere Abgrenzung der unterschiedlichen Formen von Cyberabwehrmaßnahmen stellt einen wichtigen ersten Schritt dar, um aus rechtlicher Sicht die Grenze zwischen rechtmäßigem und unrechtmäßigem Verhalten im Cyberspace zu bestimmen.[10]

Tanya Gärtner (M. lur.) ist wissenschaftliche Mitarbeiterin in der Abteilung" IT Law & Interdisciplinary Privacy Research" am Fraunhfoer SIT und forscht im ATHENE Forschungsbereich „Legal Aspects of Privacy and IT Security" (LeAP).

Literaturverzeichnis

- Arnauld, Andreas von: Völkerrecht, 3. Auflage, Heidelberg 2016.

- Delerue, François: Cyber Operations and International Law, Cambridge 2020.

- Denning, Dorothy E./Strawser, Bradley J.: Active Cyber Defense: Applying Air Defense to the Cyber Domain, S. 193 - 210. In: Perkovich, George/Levite. Ariel E. (Hrsg.): Understanding Cyber Conflict. Fourteen Analogies, Washington 2017.

- Gärtner, Tanya/Selzer, Annika, Begriffsverwirrung verhindern: Was Maßnahmen der Aktiven Cyberabwehr sind - und was nicht, über: https://background.tagesspiegel.de/cybersecurity/begriffsverwirrung-verhindern-was-massnahmen-aktiver-cyberabwehr-sind-und-was-nicht.

- National Institute of Standards and Technology, Intrusion, Glossary, über: https://csrc.nist.gov/glossary/term/intrusion#:~:text=Definition(s)%3A,See%20intrusion.

- Shulman, Haya/Waidner, Michael, ATHENE Whitepaper, Aktive Cyberabwehr, über: https://www.athene-center.de/fileadmin/Downloads/aktive-cyberabwehr.pdf .

[10] Gärtner/Selzer, Begriffsverwirrung verhindern: Was Maßnahmen Aktiver Cyberabwehr sind – und was nicht.

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Alternativen zum „Hackback“?
Staatliche Cybersicherheitsangriffe aus Sicht des Völkerrechts