8. Abschließende Zusammenfassung

Zusammenfassend ist festzustellen, dass die Entwicklung und Herausbildung von Staatenpraxis für die künftige Anwendung und Auslegung des Völkerrechts auf *Cyberwarfare* entscheidend ist. Die vorgestellte Cyberstrategie Deutschlands spiegelt in den allermeisten Fragen das geltende Recht wider. Für die USA gilt dies allerdings nur mit Abstrichen, da diese mitunter eine progressive Auffassung vertreten, insbesondere was das Selbstverteidigungsrecht betrifft.[84] In der Zukunft sollte weiter die Erarbeitung einer internationalen Strategie im Rahmen von internationalen Organisationen, Staatenverbänden und Militärbündnissen angestrebt werden, um eine weitest mögliche Rechtssicherheit und Rechtsgeltung zu erreichen. Die technologische Entwicklung von Cybermitteln und damit auch *Cyberwarfare* wird sich nicht aufhalten lassen, weswegen eine bestmöglichste Vorbereitung, die Absteckung von Grenzen und die Festlegung eines einheitlichen rechtlichen Rahmens von höchster Bedeutung sind.

84 Schmitt (Anm. 14), S. 23; Tallinn Manual (Anm. 2), S. 54, S. 58ff.

Internationale Kooperationsrichtlinien – ein Ausweg aus dem Attributionsdilemma

Thomas Reinhold*

Abstract: The attribution is a key element for international legitimacy of national self defence against cyber attacks. In many debates, the anonymity of the internet is pointed out as a main advantage for attackers, as it successfully prevents detection and sanctioning. A more technical perspective on the infrastructures and processes of data transmission reveals possibilities for identifying attackers that may prove sufficient for attribution. The article discusses when this might be the case and argues that the internet is not a place of anonymity at all. Deficient national and international norms are identified as the main obstacles for cyber attack attribution. These findings are considered in the light of individual rights, privacy and data protection. The objective of this article is the demystification of the internet as an anonymous space for further debates and to point out the importance of the development of rules and regulations for international cooperation to a special degree.

Keywords: Cyberwarfare, international cooperation, anonymity, identification, cyber attacks, IT
Cyberkriege, internationale Zusammenarbeit, Anonymität, Identifikation, Cyberattacken, IT

1. Cyberattacken und deren Verortung

Seit 2010 der Computerwurm Stuxnet durch einen Sabotageangriff gegen das iranische Atomprogramm bekannt wurde, berichten Medien regelmäßig von größeren Hacker-Attacken, dem Diebstahl immenser Datenmengen oder Vorfällen von Computerspionage. Neben der normalen Kriminalität im Internet sorgen dabei die Angriffe staatlicher Akteure wie die langjährigen Zugriffe chinesischer Hacker auf Computersysteme der US-amerikanischen Militärindustrie (Madiant 2013) oder die Enthüllungen über US-amerikanische Hackergruppen, die weltweit Daten aus Computersystemen stehlen (Business Week 2013), zunehmend auch in den internationalen politischen Beziehungen für Beunruhigung. Dem gegenüber steht die oft widerspruchslos akzeptierte These vom Internet als einem rechtsfreien Raum mit unbekannten und anonymen Angreifern, die ihre Aktivitäten beliebig tarnen und verbergen können und sich auf diese Weise einer effektiven Strafverfolgung und der Durchsetzung internationaler Rechtsnormen entziehen. Zentrales Argument dieser Sichtweise ist die postulierte faktische Unmöglichkeit der Attribution, also die Zuordnung und Verortung der Herkunft einer Cyberattacke und die Identifikation der menschlichen Angreifer. Im Gegensatz zu diesen Annahmen bieten die technischen Grundlagen des Internets und die paketbasierte Übertragung von Informationen zwischen Computern über bestehende Netzwerke eine sehr gute Grundlage für die Identifikation von Cyberattacken. Des Weiteren stellt sich im Falle von Cyberattacken staatlicher Akteure die Frage, welcher Grad an Attribution hinreichend ist und ob für eine angemessene Reaktion eines Staates die exakte Kenntnis der Identität des menschlichen Akteurs notwendig ist. Anhand dieser Fragestellungen kann deutlich gezeigt werden, dass die aktuellen Probleme der Attribution nicht auf der vermeintlichen Anonymität des Internets beruhen. Das entscheidende Problem bei der Rückverfolgung von Angriffen sind vielmehr fehlende internationale, mit demokratischen Werten zu vereinbarende Maßnahmen zur Speicherung von Daten über Internetverbindungen, mangelnde verbindliche Regularien zu Kommunikations- und Datenaustauschkanälen sowie den Speicherfristen dieser Informationen. Unter diesen Gesichtspunkten ist die zentrale Frage des Artikels, welche Bedingungen für eine erfolgreiche Attribution von staatlichen Cyberattacken notwendig sind, welche technischen Grundlagen dafür benötigt werden und welche Anforderungen sich daraus

* Thomas Reinhold ist Diplom Informatiker (TU) und Fellow am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH); Email: reinhold@ifsh.de.
Dieser Artikel wurde einem anonymen Begutachtungsverfahren (double-blind peer reviewed) unterzogen.

insbesondere für den Bereich der internationalen staatlichen Kooperationen ergeben.

2. Die Datenübertragung im Internet

Das Internet ist ein Netzwerk aus Netzwerken, gebildet aus vielen einzelnen, miteinander über die unterschiedlichsten Kanäle verbundenen Computersystemen. Diese Netzwerke werden in aller Regel von privatwirtschaftlichen Anbietern betrieben und sind über zentrale Knotenpunkte miteinander verbunden. Eine Verbindung und Datenübermittlung zwischen zwei beliebigen Geräten über das Internet besteht in der Übertragung von Informationen über viele Netzwerke und Computersysteme hinweg. Die zu übertragenden Informationen werden dabei aufgeteilt in kleine Datenpakete, die einzeln versandt und am Zielort wieder zusammengefügt werden. Jedes Datenpaket wird dabei ähnlich einem Brief mit einem digitalen Umschlag versehen, der neben weiteren Angaben auch zwingend mit der Absender- und der Empfängeradresse versehen ist. Computersysteme, die für die Weiterleitung von Datenpaketen zuständig sind, lesen diese Adressangaben und verwenden sie für die korrekte Zustellung oder die Weiterleitung des Datenpakets. Die Informationen dieser Computersysteme über die Übertragung eines Pakets einer bestimmten Größe von Sender A zu Empfänger B zu einem bestimmten Zeitpunkt werden als Verbindungsdaten bezeichnet. Abhängig von dem jeweiligen Betreiber des Computersystems, dessen lokaler Jurisdiktion sowie der Funktion der Daten – wie beispielsweise für Abrechnungszwecke bei Internetprovidern – werden diese Verbindungsdaten sofort verworfen oder wenige Tage bis zu einigen Monaten lang gespeichert.

Ein weiteres Prinzip der Datenübertragung im Internet besteht in der Verwendung der sogenannten Internet-Protocol-(IP)-Adressen für die Identifikation und Adressierung von einzelnen Computersystemen und Computernetzwerken. Jedes Computersystem – vom Smartphone bis zum Industrie-Server – hat innerhalb des Netzwerkes, in dem es sich befindet, eine eigene IP-Adresse und ist darüber eindeutig identifizierbar. IP-Adressen sind dabei numerische Angaben in Form von vier Zahlen, von 0 bis 255, die durch einen Punkt getrennt werden[1]. Die Menge der insgesamt weltweit verfügbaren IP-Adressen ist aufgrund dieses Formats begrenzt und IP-Adressen werden daher von der Organisation IANA (Internet Assigned Numbers Authority) zentral verwaltet und verteilt. Nach demselben Adressierungsprinzip einzelner Geräte sind auch die unterschiedlichen, miteinander verbundenen Sub-Netzwerke über eindeutige IP-Adressierungen[2] identifizierbar. Die Adressinformationen der übertragenen Datenpakete enthalten also stets die Identifikationsangaben des Absender- und Zielnetzwerks sowie die Identifikationsadressen des Absender- und Zielgeräts innerhalb dieser Netzwerke. Dieser Mechanismus ermöglicht eine sukzessive Übertragung und finale Zustellung von Datenpaketen über die unterschiedlichen Zwischenschritte hinweg. Des Weiteren kann ein Zielgerät die Herkunft eines Datenpakets anhand der Identifikationsdaten bestimmen, da diese Informationen für die Rücksendung von angeforderten Daten notwendig sind.

Ein dritter, wesentlicher Aspekt des Internets besteht darin, dass jegliche Computersysteme bei aller empfundenen Virtualität des Internets stets reale physikalische Standorte haben, sich damit also auch de facto immer innerhalb von Staatsgrenzen und Jurisdiktionen befinden. Gleiches gilt für übertragene Datenpakete, da diese sich während der Datenübertragung im Speicher eines oder – im Falle des exakten Zeitpunkts der Signalübermittlung per Kabel oder Funk – im Speicher zweier Computersysteme befinden. Aufgrund der zentralen Verwaltung der IP-Adressen und dem damit verbundenen Registrierungsprozess lassen sich anhand von IP-Adressen das Netzwerk, innerhalb dessen sich ein Computersystem befindet, der Betreiber[3] dieses Netzwerks und auch relativ genau der konkrete Standort des Geräts bestimmen[4].

Ausgehend von diesen Grundprinzipien basieren auch Attacken auf Computersysteme, wie jegliche normale Internetverbindungen, auf diesen Regeln der Datenübertragung. Auch wenn es unterschiedlichste Methoden von Cyberangriffen gibt, versuchen Angreifer in aller Regel Zugriff auf Zielsysteme zu erlangen und Datenkanäle zu etablieren, über die der Angriff und die dabei verwendete Schadsoftware gesteuert und entwendete Daten kopiert werden können[5]. Derartige Zugriffe erfolgen in aller Regel nicht über direkte Verbindungen von den persönlichen Computern der Angreifer aus, Angreifer verwenden auf dem Weg zwischen sich und ihrem Ziel vielmehr weitere Computer als Zwischenschritte, um ihre Identität zu verschleiern. Solche Zwischenschritte können zum einen fremde, im Vorfeld mit Hilfe von Software-Sicherheitslücken unberechtigt unter Kontrolle gebrachte Computersysteme sein, die vom eigentlichen Eigentümer unbemerkt angewiesen werden, bestimmte Verbindungen aufzubauen und Operationen durchzuführen. Eine weitere übliche Technik besteht in der Verwendung sogenannter Command-und-Control-Server (C&C). Dabei handelt es sich um angemietete Computersysteme, die als Steuerungszentralen mit spezieller Software für die eigentliche Attacke eingesetzt werden sowie als Sammelpunkt für kopierte Daten und entwendete Informationen dienen. Ein exemplarischer Cyberangriff erfolgt beispielsweise, indem ein Angreifer zuerst mit Hilfe von infizierten E-Mailanhängen, modifizierten Web-Seiten oder ähnlichem Schadsoftware auf dem Computersystem des Opfers installiert und sich damit eine „Hintertür" in dessen System schafft. Für die weitere Steuerung der Attacke loggt sich der Angreifer auf seinem C&C-Server ein und erteilt über die zentrale Steuerungssoftware seine Befehle. Diese werden an alle infizierten Opfer-Systeme verteilt und dort von der installierten Schadsoftware ausgeführt. Im Falle von Datendiebstahl würden dann die gesammelten Daten an den C&C-Server zurückgesendet, dort gespeichert und schließlich zum Privatrechner der Angreifers transferiert. Um die entste-

1 Bspw. identifiziert die IP-Adresse 88.215.213.26 einen der Server von tagesschau.de.

2 Im Detail werden bei der Adressierung von Netzwerken keine eindeutigen IP-Adressen, sondern eindeutige Adress-Räume für die Identifikation verwendet. Dies wird hier aus Gründen der Anschaulichkeit vereinfacht dargestellt. Lienemann 2010 bietet eine gute genauere Darstellung der IP-Adressierung und der Transmission Control Protocol (TCP)-Datenübertragung.

3 Die Registrierungsdaten lassen sich unter anderem bei der DENIC über WHOIS abfragen: http://www.denic.de/domains/whois-service.html.

4 Beispielsweise über die Webseite http://ipcim.com/en/?p=where.

5 Auf eine detailierte Darstellung der verschiedenen Formen von Cyberattacken wird an dieser Stelle im Sinne der exemplarischen Darstellung verzichtet. Moreno 2011 bietet eine gute Übersicht über diese Details.

henden Datenströme zu tarnen und die eigene Identität zu schützen, ergreifen Angreifer in aller Regel unterschiedliche Maßnahmen, wie die Verschlüsselung der übertragenen Daten. In diesem und den meisten weiteren Fällen bleiben jedoch die eigentlichen, für die Datenübermittlung notwendigen Adressinformationen unberührt, sodass weiterhin aussagekräftige Verbindungsdaten anfallen. Eine besondere Möglichkeit der Identitätsverschleierung besteht in der Verwendung eines Anonymisierungsnetzwerks wie TOR[6]. Das Prinzip derartiger Netzwerke basiert auf dem Transfer von Datenverbindungen über viele spezielle Anonymisierungsknotenpunkte hinweg, wobei die entscheidende Ursprungs-Herkunftsadresse eines Datenpakets effektiv verschleiert wird[7]. Angriffe staatlicher Akteure über das TOR-Netzwerk sind jedoch bisher noch nicht vorgekommen und aufgrund einiger spezifischer technischer Besonderheiten des TOR-Netzwerks wenig praktikabel. Darüber hinaus demonstrieren sowohl die Erfinder von TOR (Torproject 2009) als auch einige der veröffentlichten Dokumente aus dem Fundus des NSA-Whistleblowers Edward Snowden (Schneier 2013), dass Datenverbindungen über das TOR-Netzwerk unter bestimmten Voraussetzungen überwachbar und Kommunikationspartner trotz Anonymisierungssoftware identifizierbar sind. In jedem Fall stellen Angriffe über das TOR-Netzwerk eine Besonderheit dar, auf die hier im Detail nicht näher eingegangen werden kann.

3. Attribution als Schlüssel für die Verantwortung staatlichen Handelns

Angesichts steigender Zahlen von Cyberattacken, dem verstärkten militärischen Engagement von Staaten im Internet und der Aufnahme von Cyberattacken in nationale Sicherheitsdoktrinen (Lewis 2011) spielt die Frage der Attribution neben Aspekten der Strafverfolgung zunehmend im internationalen politischen Kontext eine wichtige Rolle. Zum einen sind Staaten dem internationalen Recht zufolge mitverantwortlich für völkerrechtswidrige Handlungen, die auf ihrem Hoheitsgebiet oder von ihren Staatsbürgern durchgeführt werden, und angehalten geeignete juristische und exekutive Kontroll- und Gegenmaßnahmen aufzubauen und zu ergreifen (UN 2001).[8] Dieses Prinzip der nationalen Verantwortlichkeit ist umso relevanter, wenn die Souveränität[9] anderer Staaten beeinträchtigt wird. Die Anwendbarkeit dieser und weiterer etablierter verbindlicher Normen des internationalen Völkerrechts auf die neue Domäne des Internets wird gegenwärtig breit diskutiert. Insbesondere die Aspekte des Rechts eines Staates zur Selbstverteidigung in Reaktion auf einen bewaffneten Angriff sind dabei stark umstritten, da die Rechtsnorm die zweifelsfreie Kenntnis des Angreifers – also die Attribution des Cyberangriffs zu diesem – zur legitimierenden Bedingung macht. Eine der wichtigsten Arbeiten, die sich der Übertragung bestehender Rechtsnormen auf die neue Domäne Internet widmet, ist das von unabhängigen Experten im Namen des NATO-Exzellenz-Zentrums (Cooperative Cyber Defence Centre of Excellence, CCD COE) erarbeitete und Anfang 2013 veröffentlichte „Tallin Manual“ (Nato 2013). Die Experten kommen darin unter anderem zu dem Schluss, dass bereits Spionage oder Sabotageakte unter Umständen das internationale Souveränitätsprinzip von Staaten verletzten können. Auch hinsichtlich der Frage des Rechts auf staatliche Selbstverteidigung kommt die Expertengruppe zu dem Schluss, dass Cyberattacken in ihrer Wirkung durchaus dem “use of force” klassischer Waffen entsprechen und die Tragweite eines bewaffneten Angriffs im Sinne des Kriegsvölkerrechts erreichen können, ohne jedoch eine exakte Schwelle des Schadensausmaßes zu definieren[10]. Über die Auslegung zur Verhältnismäßigkeit „angemessener Reaktionen“ auf Cyberbedrohung scheiden sich jedoch weiterhin die Geister und es ist international insbesondere stark umstritten, ob Bedrohungen durch Cyberattacken beispielsweise mit Hilfe konventioneller Waffen abgewehrt werden dürfen.

4. Internationale Rückverfolgung von Angriffen

Wie kann also Attribution bei Cyberattacken realisiert werden? Herb Lin (Lin 2011), Clark et. al. (Clark 2010) und auch die UN-Organisation UNODC (United Nations Office on Drugs and Crime) (UNODC 2012) argumentieren, dass für die Frage der Attribution in einem konkreten Fall zum einen die genaue Eingrenzung des Begriffs „Angreifer“ sowie die Frage nach der Reaktion auf diese Cyberattacke entscheidend ist: „Perpetrator of an attack has different meanings: the machines between attacker and attackee (hubs), the machine of the attacker itself, the geographical location, the person who launched the attack, the nation or the entity under whose auspices the individual acted [..] Depending on what you would like to do about the attacks defines what kind of attribution you need (e.g.: mitigate the pain as soon as possible: know the machines, prosecute/take actor into custody: know the operator)“ (Lin 2011). Dieser Logik folgend ist bei Fällen von Cyberattacken mit mutmaßlich staatlichen Akteuren die Kenntnis des eigentlichen menschlichen Akteurs weniger relevant als vielmehr die Kenntnis und Identifikation des Ursprungsnetzwerks als wichtiges Indiz auf den dahinter stehenden staatlichen Akteur. Wie bereits dargestellt, kann anhand von gespeicherten Verbindungsdaten aus Sicht der technischen Grundlagen eine solche Identifikation vorgenommen werden. Sofern es möglich ist, Cyberattacken zeitnah, im Idealfall während ihrer Durchführung, aufzudecken, können aktive Datenverbindungen zwischen den Angreifern und den Zielsystemen sowie Bestandteile der verwendeten IT-Infrastruktur überwacht und Verbindungsdaten für die Identifikation gesammelt werden. Tatsächlich besteht ein wichtiger Bestandteil bei der Auswertung von Cyberattacken durch IT-Forensiker in der Analyse sichergestellter Verbindungsdaten, dem Einrichten von sogenannten Honey-pots[11] und darüber der Identifikation von Command-und-Control-Servern sowie dem Sicherstellen und Auswerten dieser Geräte.

6 TOR – The Onion Router, https://www.torproject.org/.
7 http://de.wikipedia.org/wiki/Tor_(Netzwerk)#Arbeitsweise bietet eine gute Darstellung dieser technischen Funktion.
8 Vgl. Resolution 56/83 der UN-Generalversammlung betreffend Staatenverantwortlichkeit bei völkerrechtswidrigen Handlungen (28.01.2002).
9 Zur staatlichen Souveränität siehe UN Charta Art. 2 (7).
10 Vgl. mit dem Beitrag von Tassilo Singer in diesem Heft.
11 Als Honey-pots werden Computersysteme bezeichnet, die als Falle für Angreifer mit gefälschten und scheinbar besonders relevanten Daten in einem Zielsystem aufgebaut werden. Diese Systeme werden dabei genau überwacht und jegliche Datenverbindungen sowie Interaktionen von Nutzern aufgezeichnet.

Betrachtet man die bisherigen Vorfälle von Cyberattacken wie FLAME[12] oder ROCRA[13] mit mutmaßlich staatlichen Akteuren wird deutlich, dass diese oft über mehrere Jahre hinweg durchgeführt (Lindner 2011) und dabei in den meisten Fällen entdeckt, wenn auch zumeist nicht sofort als Angriffe staatlicher Akteure erkannt wurden. Anhand einer Überwachung dieser Angriffe sowie dem Sammeln und Auswerten von Verbindungsdaten der weiteren verwendeten Übertragungszwischenschritte wäre es möglich gewesen, die Gesamtverbindung systematisch Schritt für Schritt, von Netzwerk zu Netzwerk, von Computer zu Computer bis zu ihrem Ursprung zurückzuverfolgen. Ein im Februar 2013 veröffentlichter Bericht der US-amerikanischen IT-Forensik Firma Madiant (Madiant 2013) hat darüber hinaus einen weiteren, pragmatischen Weg zur Attribution insbesondere langfristiger Cyberattacken verdeutlicht. Die Ergebnisse und Untersuchungen der Organisation, die seit 2006 mit der Untersuchung von Cyberattacken gegen große US-Konzerne beauftragt waren, zeigen, dass die Attribution von Cyberattacken auch rückwirkend möglich ist, wenn die Menge der sichergestellten Computersysteme und die für Analysen verfügbaren Daten hinreichend groß sind, um Datenverbindungen und Zugriffe der Angreifer wiederherzustellen und Muster im Verhalten der Angreifer aufzudecken. Der Bericht umfasst die Untersuchung einer Vielzahl von Cyberattacken und verbindet die Analysen mit klassischen forensischen und kriminologischen Methoden wie der Suche nach den mutmaßlichen Hackern in einschlägigen Online-Foren oder bei Social-Media-Diensten. Anhand dieser Indizien können die Urheber des Berichts eine chinesische Hacker-Gruppe als Ursprung der untersuchten Cyberattacken identifizieren und schlüssig darlegen, dass es sich dabei mutmaßlich um eine Militäreinheit (PLA 61398) der chinesischen Volksbefreiungsarmee handelt.

Wie dargestellt wurde, existieren aufgrund der technischen Grundlagen der Internet-Datenübertragung die für eine Attribution notwendigen Verbindungsdaten und könnten für eine Analyse erfasst und gespeichert werden. Das wesentliche Problem bei dieser Rückverfolgung besteht demzufolge weniger in der Verfügbarkeit als vielmehr in der kurzen Zeitspanne eines legalen Zugriffs auf die Verbindungsdaten und die beteiligten Computersysteme sowie der dafür benötigten Kooperation mit den Betreibern der Computernetzwerke. Diese befinden sich aufgrund der globalen Struktur des Internets entweder außerhalb der eigenen staatlichen Jurisdiktion oder es gibt unklare Gesetzeslagen zu Fristen und der Rechtmäßigkeit der Datenspeicherung sowie deren Weitergabe an nationale und internationale Strafverfolgungsbehörden. Auf diese Weise gehen wichtige Informationen über Datenverbindungen verloren, die durch einheitliche Regularien und etablierte reaktionsschnelle Kooperationsmechanismen sichergestellt werden könnten. Angesichts der Relevanz der Verbindungsdaten und deren Bedeutung für die Attribution darf die vollständige Datenspeicherung über viele Monate hinweg, wie es unter anderem der EU-Ansatz zur sogenannten Vorratsdatenspeicherung[14] vorsieht, jedoch nicht die Konsequenz dieser Überlegungen sein. Die Totalüberwachung des digitalen Verhaltens ganzer Gesellschaften kann aus der Sicht des menschenrechtlichen Anspruchs auf Achtung der Privatsphäre, der informationellen Selbstbestimmung und einer Umkehrung der Unschuldsvermutung keine Lösung für das Problem der Attribution darstellen (BVerfG 2010). Auch die Erhebung dieser Daten durch Nachrichtendienste im Zeichen der Terrorbekämpfung ist hinsichtlich ihrer einschneidenden Bedeutung für freiheitliche und demokratische Maßstäbe sehr umstritten[15]. In den Diskussionen zur deutschen Umsetzung der Vorratsdatenspeicherungsrichtlinie und der Kritik an einer Totalüberwachung wurden daher alternative Ansätze wie das sogenannte Quick-Freeze-Verfahren vorgeschlagen. Dieses Verfahren bezieht sich auf einen Vorschlag Scott Charneys, dem damaligen Vorsitzenden der G-8-Arbeitsgruppe zum Thema High-Tech-Kriminalität aus dem Jahr 1999. Der Ansatz des Quick-Freeze-Verfahrens besteht in der kurzfristigen und zeitlich eng begrenzten Zwischenspeicherung anhand von Indizien gezielt ausgewählter und gefilterter Verbindungen, um diese Datenströme zeitversetzt analysieren zu können. Voraussetzung für dieses Verfahren ist der Verdacht oder die Kenntnis laufender Cyberattacken die, wie dargestellt und anhand der vergangenen Fälle deutlich geworden, bei langfristigen staatlich militärischen Cyberoperationen zumeist gegeben ist.

5. Klare Kooperationsrichtlinien sind das Gebot der Stunde

Das entscheidende Problem der Attribuierbarkeit von Cyberattacken stellen also weniger die technischen Grundlagen des Internets, als vielmehr die für die Analysen notwendige, zeitnahe Erfassung der Verbindungsdaten dar. Mit dem Quick-Freeze-Verfahren steht jedoch eine geeignete, menschenrechtlich vertretbare Lösung für die Speicherung dieser Informationen und die potenzielle Weitergabe an nationale und internationale Strafverfolger zur Verfügung. Derartige Ansätze benötigen jedoch zum einen international einheitliche Regularien zur Umsetzung der dafür benötigten technischen Grundlagen, die Implementierung dieser Regularien in nationalen Gesetze und deren konkrete Umsetzung bei den technischen Dienstleistern der weltweiten Internet-Infrastrukturen. Des Weiteren bedarf es effektiver internationaler Kommunikationskanäle und -hierarchien und der Einrichtung von staatlichen Kontaktstellen, um im Falle von Cyberattacken Quick-Freeze-Verfahren bei Internetdienstleistern entlang der kompletten Datenübertragungsketten von Cyberattacken anzuordnen und die relevanten Verbindungsdaten zusammenzutragen. In der Europäischen Union ist die Bedeutung von derartigen Harmonisierungsmaßnahmen

12 Analyse der C&C-Server von FLAME, https://www.securelist.com/en/blog/750/Full_Analysis_of_Flame_s_ Command_Control_servers.

13 Analyse zu ROCRA, auch bekannt unter der Bezeichnung "Roter Oktober", http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation.

14 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU L 105, 54 vom 13. April 2006.

15 Siehe unter anderem das Schlussplädoyer des Generalanwalts Pedro Cruz Villalón im Verfahren gegen die EU-Richtlinie zur Vorratsdatenspeicherung vor dem EuGH vom 12.12.2013: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=187576.

im Kampf gegen Cyberattacken erkannt worden. Erste Ansätze wie einheitliche Regelungen für nationale Meldepflichten und Meldestrukturen sowie klare Verantwortlichkeitshierarchien bei der Aufdeckung von Bedrohungen sollen helfen, Cyberattacken zu erkennen, nationale Autoritäten zu unterrichten, die Informationen zu Bedrohungen an internationale Partner weiterzugeben und gemeinsam zu reagieren. Ein wichtiger Schritt besteht dabei in der Einrichtung oder dem weiteren Ausbau sowie der internationalen Vernetzung von nationalen Informationszentralen, sogenannten CERTs (Computer Emergency Response Teams), die über hierarchische Meldekanäle von Bürgern, Industrien und Behörden sicherheitsrelevante Informationen zentral zusammenführen und verteilen. Derartige Maßnahmen weisen in die richtige Richtung, reichen aber weiterhin nicht für eine rasche Rückverfolgung aus. Praxiserfahrungen der internationalen Kooperationsmechanismen bei der Verfolgung von Kriminalität im Internet zeigen, dass eine effektive und zeitnahe Kooperation der relevanten Organisationen nach wie vor oft an bürokratischen Hindernissen und Verwaltungshierarchien scheitert. Die Entwicklung handlungsfähiger Strukturen ist daher eines der wichtigen Ziele, wie sie beispielsweise von der Europäischen Agentur für Netz- und Informationssicherheit[16] (European Union Agency for Network and Information Security, ENISA) oder den Diskussionen um die stärkere Einbindung von UN-Gremien in Form der Internationalen Fernmeldeunion[17] (International Telecommunication Union, ITU) in Verwaltungs- und Regulierungsfragen des Internet betrieben werden. Entscheidend ist es, für die weiteren Diskussionen festzuhalten, dass Attribution aus technischer Sicht auch im Internet möglich ist, relevante Daten aus technischer Sicht zur Verfügung stehen und der Angreifer somit nicht jener große Unbekannte sein muss, der – teils aus Unkenntnis der technischen Grundlagen, teils aus politischem Kalkül heraus – nur zu oft gezeichnet wird. Inwiefern diese Sichtweise auch im politischen Rahmen aufgegriffen und konstruktiv national und international in Form stärkerer Zusammenarbeit umgesetzt wird, bleibt jedoch abzuwarten.

Quellen

Businessweek, 2013, "How the U.S. Government Hacks the World", New York, http://www.businessweek.com/articles/2013-05-23/how-the-u-dot-s-dot-government-hacks-the-world (Stand 21.01.2013)

BVerfG, 2010, Urteil des Bundesverfassungsgerichtes gegen die §§113a, 113b des Telekommunikationsgesetzes in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl I S. 3198), Karlsruhe

Clark, David D./Landau, Susan, 2011, "The Problem isn't Attribution; It's Multi-Stage Attacks", MIT Computer Science and Artificial Intelligence Laboratory, Cambridge

Lewis, James A./Timlin, Katrina, 2011, "Cybersecurity and Cyberwarfare – Preliminary Assessment of National Doctrine and Organization", Center for Strategic and International Studies, Washington

Lienemann, Gerhard/Larisch, Dirk, 2010, "TCP/IP Grundlagen und Praxis", Heise Verlag, Hamburg

Lin, Herb, 2011, "On Attribution and Defense", International Conference on Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Berlin, Germany

Lindner, Felix, 2011, "Military Grade Hacking - This Is Not Cyber Crime", International Conference on Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Berlin, Germany

Madiant, 2013, "APT1 Exposing One of China's Cyber Espionage Units", Washington, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (Stand 21.01.2013)

Moreno, Francisca, 2011, "Security 101: Vulnerabilities" und "Security 101: Attack vectors", McAfee Labs, http://blogs.mcafee.com/mcafee-labs/security-101-vulnerabilities-part-1, http://blogs.mcafee.com/mcafee-labs/security-101-vulnerabilities-part-2 (Stand 21.01.2013)

NATO CCDCOE, 2013, "The Tallinn Manual on the International Law Applicable to Cyber Warfare", Tallin

Torproject, 2009, "One cell is enough to break Tor's anonymity", blog.torproject.org, https://blog.torproject.org/blog/one-cell-enough (Stand 21.01.2013)

Schneier, Bruce, 2013, „How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID", schneier.com/blog, https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html (Stand 21.01.2013)

UN International Law Commission, 2001, „Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83", New York

UNODC, 2012, „The use of the Internet for terrorist purposes", United Nations Office on Drugs and Crime, Wien

16 EU Cybersecurity Strategy & Directive 2013: http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced.

17 Draft of the proposed revisions of the international telecommunication regulations: http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf.