BLAME GAME IM CYBERSPACE

INFORMATIONSTECHNIK ALS WAFFE?

SEBASTIAN HARNISCH & KERSTIN ZETTL

Konflikte zwischen Staaten müssen sich nicht in blutigen Kriegen äußern, sondern können auch versteckter im virtuellen Raum der Informationstechnologie ausgetragen werden. Die Bandbreite sogenannter Cyberangriffe ist groß und reicht vom Diebstahl geistigen Eigentums über Desinformationskampagnen und Wahlmanipulation bis zu Eingriffen in die Infrastruktur eines gegnerischen Landes – indem Kraftwerke durch einen Hackerangriff abgeschaltet werden. Mithilfe eines weltweit einmaligen Datensatzes untersuchen Heidelberger Politikwissenschaftlerinnen und Politikwissenschaftler das Verhalten von Demokratien und Autokratien in solchen Cyberkonflikten.

KERSTIN ZETTL (M.A.) ist seit 2019 wissenschaftliche Mitarbeiterin in einem von der Deutschen Stiftung Friedensforschung geförderten Forschungsprojekt zu Cyberkonflikten unter der Leitung von Sebastian Harnisch am Institut für Politische Wissenschaft der Universität Heidelberg. Gleichzeitig arbeitet sie an ihrer Dissertation zum Vergleich autokratischer und demokratischer Cyber-Proxy-Strategien. Zuvor studierte sie Politikwissenschaft, Psychologie und Bildungswissenschaft an der Universität Heidelberg.

Kontakt: kerstin.zettl@ipw.uni-heidelberg.de

A

Als im US-Präsidentschaftswahlkampf 2016 der Öffentlichkeit nach und nach E-Mail-Inhalte zugespielt wurden, die für die Demokratische Partei kompromittierend waren, lag die Zuschreibung – auch Attribution genannt – einer Wahlbeeinflussung durch Russland auf der Hand. Private IT-Firmen und ungenannte Regierungsquellen deuteten in Richtung des Kreml. Die russische Regierung, so der Vorwurf, habe zwei Hackergruppierungen mit der Infiltrierung der Netzwerke des „Democratic National Committee" (DNC) beauftragt – sogenannte „Cyberproxys", wie staatlich beauftragte oder unterstützte nichtstaatliche Akteure in Cyberkonflikten genannt werden. Eine offizielle Zuschreibung der US-Regierung folgte zeitnah allerdings nicht. Erst im Oktober 2016 und damit mehrere Monate nach dem Vorfall kam es zu einer offiziellen Erklärung der US-Regierung, in der Russland der Wahlbeeinflussung beschuldigt wurde.

Das Zögern der Obama-Administration steht für einen größeren Trend: Demokratische Regierungen schrecken regelmäßig davor zurück, bekannt gewordene Cyberangriffe auf ihr Land bestimmten Tätern öffentlich zuzuschreiben. Geschieht dies doch, werden bislang selten fremde Regierungen direkt als Angreifer genannt, stattdessen wird von „staatlich gesponserten" Cyberangriffen gesprochen. Das zeigen die Daten unseres Forschungsprojekts „Sicherheit durch Verschleierung: Warum Regierungen Proxys in Cyberkonflikten einsetzen" am Institut für Politische Wissenschaft.

Der Heidelberger Cyberkonfliktdatensatz HD-CY.CON

In dem von der Deutschen Stiftung Friedensforschung geförderten Projekt untersuchen wir, ob und inwiefern sich Autokratien und Demokratien im Cyberkonfliktverhalten, insbesondere dem Gebrauch von Proxys, unterscheiden. Aufbauend auf Untersuchungen, die durch das Field of Focus 4 der Universität Heidelberg gefördert wurden, starten wir mit der These, dass Autokratien Proxys für Cyberangriffe nutzen, während Demokratien diese primär zur Attribution einsetzen, also zur Identifizierung des Angreifers. Indem die Zuschreibung an IT-Firmen ausgelagert wird, kann vermieden werden, dass eine demokratische Regierung durch die selbst getätigte Verantwortungszuweisung unter öffentlichen Handlungsdruck gerät: Wo kein Angreifer, da kein

PROF. DR. SEBASTIAN HARNISCH hat seit 2007 eine Professur für Internationale Beziehungen und Außenpolitik am Institut für Politische Wissenschaft der Universität Heidelberg inne. Zuvor forschte und lehrte er unter anderem an Universitäten in Trier, München, Peking (China), New York (USA), Seoul (Südkorea) und Tokio (Japan). Seine Forschungsprojekte und Publikationen umfassen die Vergleichende Außen- und Sicherheitspolitik, Theorien der Internationalen Beziehungen, Nonproliferation, Netzpolitik und Klimawandel. Mit der Thematik der Attribution von Cyberangriffen beschäftigt er sich besonders seit 2019 im Rahmen eines von der Deutschen Stiftung Friedensforschung geförderten Forschungsprojektes.

Kontakt: sebastian.harnisch@ipw.uni-heidelberg.de

„Aufgrund ihrer großen digitalen Angriffsflächen scheuen demokratische Staaten längerfristige Cyberkonflikte, welche durch eigene Gegenmaßnahmen erst ausgelöst werden können.“

Täter. Für Cyberangriffe auf Demokratien könnte somit gelten: Wo kein Täter, da keine Strafverfolgung und kein Richter.

Im Rahmen des Forschungsprojektes erstellen wir zunächst einen umfassenden, weltweit einmaligen Datensatz: HD-CY.CON. Dieser erfasst sowohl die beschriebene offensive Proxynutzung autokratischer Staaten als auch die vermutete defensive, auf Attribution ausgerichtete Proxynutzung von Demokratien. Der Ansatz grenzt sich von bereits existenten Cyberkonfliktdatensätzen durch seinen besonderen Fokus auf den Aspekt der Attribution ab: Wer identifiziert regelmäßig welche Akteure als vermeintliche Täter? Liegt hierbei ein Muster gemäß den Angriffstypen (Cyberkriminalität, -spionage, -konflikte) und ihrer Intensitäten vor? Werden die Zuschreibungen von dritten Akteuren regelmäßig angefochten? So erfassen wir bislang für die Jahre 2000 bis 2017 Anzahl, Art und Attribution von Cyberangriffen und -gegenangriffen in ihrer Dynamik und analysieren sie.

Attribution ist der Anfang von allem

Theoretisch folgen wir mit den beschriebenen Überlegungen den bisherigen Forschungsarbeiten zum sogenannten Attributionsproblem: In der Cybersicherheitsforschung versteht man darunter jene stark erschwerte Verantwortungszuweisung im Falle von Cyberattacken, die auf die technische Komplexität und die politischen Verschleierungsmöglichkeiten im Internet zurückgeht. Ohne Attribution ist jedoch auch kein zielgerichtetes Handeln möglich, beispielsweise die Abschreckung von Angriffen durch die glaubwürdige Androhung von Gegengewalt. Politische Verschleierungsstrategien dienen dazu, je nach Regimetypus die Konsequenzen eigener, fremder oder beauftragter Handlungen zu vermeiden. So können in konventionellen Konflikten unterlegene Autokratien mit der Beauftragung von Proxys die Kosten von Gegenmaßnahmen entweder auf die Beauftragten abwälzen oder solche Kosten gänzlich vermeiden. Demokratien dagegen können als Opfer von Angriffen die Verantwortungszuschreibung IT-Firmen überlassen und somit gesellschaftliche Forderungen nach Gegenmaßnahmen (zunächst) vermeiden.

Aufgrund ihrer großen digitalen Angriffsflächen scheuen demokratische Staaten bislang längerfristige Cyberkonflikte, die durch eigene Gegenmaßnahmen erst ausgelöst werden können. Zwar haben auch demokratische Regierungen nach Cyberangriffen ein starkes Interesse daran, politische Verantwortung zuzuweisen. Doch sind sie im Falle einer offiziellen Zuschreibung durch gesellschaftlichen Druck eher gezwungen, auch eine Reaktion folgen zu lassen – und diese muss sich, aufgrund ihrer rechtsstaatlichen

„Um Drohungen und Abschreckung im Cyberraum zu kommunizieren, muss der Drohende sich und sein Drohpotenzial zu erkennen geben."

Standards, mit transparenten und substanziellen technischen Beweisen unterfüttern lassen. Zudem besteht kein internationaler Konsens darüber, wie allgemeingültige Attributionsstandards zwischen Staaten aussehen sollten, wer über deren Einhaltung befindet und welche Form der Reaktion auf welche Art von Cyberangriff völkerrechtlich angemessen ist. Schon allein die Regeln für notwendige Cyberschutzmaßnahmen und die Meldepflicht bei Attacken auf Wirtschaftsunternehmen, wozu auch kritische Infrastruktur gehören kann, sorgen für Kopfzerbrechen: So gibt es in vielen Staaten Auseinandersetzungen darüber, wer die Kosten von Cyberangriffen tragen sollte – der Staat oder die Unternehmen. Kurz: Es bestehen diverse Anreize für demokratische Regierungen, offizielle Zuschreibungen von Cyberangriffen zu vermeiden.

Attribution und Cyberforensik

In seiner Entstehungsgeschichte zielte das Internet als „Netzwerk der Netzwerke" auf die ungehinderte Kommunikation von gleich(gesinnt)en Teilnehmern und weniger auf die zweifelsfreie Identifizierung der Kommunikationsteilnehmer. Dies beflügelte in der Gründergeneration unter anderem die Vision eines dezentralen, von staatlicher (All-) Macht losgelösten und deshalb demokratisierenden Mediums. Für potenzielle Angreifer bietet der technische Aufbau des Netzes zudem vielfältige Möglichkeiten der eigenen Identitätsverschleierung, unter anderem auch durch das sogenannte „Darknet". Drei technische Verschleierungswege sind besonders prominent: erstens immer ausgefeiltere Verschlüsselungstechniken, zweitens die Verwendung sogenannter Proxyserver – gewissermaßen „Mittler" in der Kommunikation zwischen zwei Computern, die Anfragen stellvertretend annehmen und weitergeben – zum Umleiten des mit dem Angriff verbundenen Datentransfers über Transitländer, sowie drittens die Instrumentalisierung von Botnetzen, also aus mehreren gekaperten Computern zusammengesetzten Netzwerken, die für Angriffe instrumentalisiert werden können.

Potenzielle Angreifer können daher im Cyberraum relativ leicht sicherstellen, dass ihre Angriffe unerkannt bleiben, wenn sie dies wünschen. Dies gilt vor allem bei Cyberspionageattacken, denn hier zieht der Angreifer keinen Nutzen aus dem Bekanntwerden des Angriffes oder seiner Vorgehensweise (Detektion), sondern möchte die bestehenden Hintertüren auch für künftige Angriffe offenhalten. Anders dagegen bei Cyberkonflikten mit kinetischen Effekten, das heißt physischen Folgen, verursacht durch Cyberangriffe, welche somit in ihrer Wirkung konventionellen Militärschlägen am ehesten ähneln. Ein Beispiel dafür ist die Abschaltung eines Stromkraftwerks auf fremdem Territorium im Zuge eines konventionellen Krieges, so geschehen in der Ukraine durch einer russischen Hackergruppe zugeschriebene Cyberangriffe. In solchen Fällen ist das Ziel oft nicht nur die sichtbare Wirkung, sondern auch das Bekanntwerden der Angriffsart: Der militärische Gegner soll verunsichert und damit von weiteren Eskalationshandlungen abgeschreckt werden

„Eine inhaltlich falsche Attribution kann im schlimmsten Falle eine nicht beabsichtigte Potenzierung des Konflikts nach sich ziehen.“

oder die Bevölkerung des gegnerischen Landes soll erpresst werden, um die gesellschaftliche Unterstützung für die Regierenden zu schwächen. Kurz: Um Drohungen und Abschreckung im Cyberraum zu kommunizieren, muss der Drohende sich und sein Drohpotenzial zu erkennen geben.

Zur eigenen Identitätsverschleierung sind auch sogenannte „False-Flag“-Attacken oft das Mittel der Wahl: Die Verwendung von schädigender Software – sogenannter Malware –, die in der Vergangenheit überwiegend einem bestimmten anderen Cyberangreifer zugeordnet wurde, lenkt den Verdacht auf diesen und nicht auf den eigentlichen Täter. So agierte die russische Hackergruppierung „Turla“, die jahrelang Angriffssysteme und -infrastruktur der iranischen Gruppe „Oil Rig“ nutzte. Bleibt diese Fremdnutzung im Falle schwerwiegender Angriffe – etwa mit kinetischen Folgen – unerkannt, können entsprechende Fehlattributionen verheerende Konsequenzen zeitigen: Denn je schwerwiegender der Angriff, desto stärker steht die jeweilige Regierung unter Druck, die Quelle unschädlich zu machen, Täter zu präsentieren und diese für ihr Handeln zu bestrafen. Eine inhaltlich falsche Attribution kann im schlimmsten Falle eine nicht beabsichtigte Potenzierung des Konflikts nach sich ziehen. Die ursprüngliche Konfliktpartei kann ungestört weiteragieren, während die neue ihrerseits genötigt wird, auf den „Vergeltungsangriff“ zu reagieren und damit möglicherweise einen neuen Konfliktzyklus in Gang zu setzen. Ein Überschwappen des Konfliktes in die „reale physische Welt“ lässt sich hierbei nicht ausschließen, wenn sich eine der Konfliktparteien besser gewappnet fühlt, den Konflikt in dieser Welt fortzuführen – man spricht dann von einem Online-Offline-Spillover-Effekt.

Die Rolle privater IT-Firmen

Unser Projekt geht zwar insbesondere der Frage nach, ob, wann und zu welchem Zweck Regierungen Proxys in Cyberkonflikten nutzen. Dabei darf jedoch das kommerzielle, kriminelle oder ideologische Eigeninteresse der Stellvertreter nicht vergessen werden. So produzieren in der Regel IT-Firmen Software und Codes, die dann anschließend von Staaten, von deren Proxys oder auch von autonom agierenden nichtstaatlichen Akteuren auf Sicherheitslücken – sogenannte Exploits – hin überprüft werden. War die Suche nach einem Exploit erfolgreich, kann der jeweilige Angreifer dieses schadhafte Codesegment in einer Attacke ausnutzen. Entsprechende Märkte versprechen – je nach „Güte“ der Malware – erhebliche Gewinne, abhängig von Reichweite und Wirkungsgrad der Exploits. Gleiches gilt aber auch für die Entwicklung von Schutzlösungen – unter anderem sogenannten Patches –, welche die Schadsoftware oder deren Wirkung neutralisieren. Kann ein Anbieter oder Softwareentwickler nun auf beiden Märkten Angebote unterbreiten, profitiert er zweimal: von der Entwicklung des Schwertes und der des zugehörigen Schildes. Eine Verlockung, die dazu führen könnte, dass die Märkte für Schad- und Schutzsoftware exponentiell wachsen, während zugleich innerhalb der Gesellschaft die potenziellen Angriffsflächen zunehmen, unter anderem,

weil das sogenannte Internet of Things (IOT) immer mehr „intelligente Alltagsobjekte“ miteinander vernetzt, etwa in einem per App oder Sprachbefehl steuerbaren „Smart Home“.

Politische Entscheider sind in solch dynamischen Situationen als „attribuierende Akteure“ auf möglichst vollständige Informationen angewiesen. Aufgrund der strukturellen Ungewissheiten im Cyberraum arbeiten sie indes häufig unter der Bedingung „begrenzter Rationalität“, das heißt, sie wägen die Kosten einer zusätzlichen Informationsbeschaffung gegenüber dem zu erwartenden Nutzen ab. Im Falle von politischen Zuschreibungen in Cyberkonflikten führt dies nun zu zwei Entwicklungsszenarien: Insbesondere demokratische Entscheider versuchen aufgrund der Attributionsproblematik sowie damit verbundener Eskalationsrisiken, mögliche öffentliche und direkte politische Verantwortungszuweisungen zu vermeiden. Sind die Anreize zu dieser Vermeidung für Entscheider hoch, dürfte eine hohe Dunkelziffer nicht (öffentlich) zugeschriebener Angriffe die Folge sein. Damit demokratische Gesellschaften sich hinreichend schützen, bedürfte es daher zusätzlicher Regeln, beispielsweise besonderer Meldepflichten, um das reale Ausmaß von Cyberangriffen besser zu erfassen. Im zweiten Szenario attribuieren Entscheider nur in solchen Fällen, in denen die Eskalationsrisiken und damit die potenziellen Reputationsverluste gering sind, das heißt, bei niedrigschwelligen Cyberangriffen. Sind die Forderungen nach einer starken Gegenreaktion verhalten, kann die Attribution ohne erkennbare politische Risiken erfolgen. Zum einen kann die öffentliche Zuschreibung den Angreifenden von weiteren Angriffen abschrecken, da er im Wiederholungsfall mit Sanktionen rechnen müsste. Zum anderen muss dieser Zuschreibung aber nicht zwingend eine konkrete Erwiderung, also ein Gegenangriff folgen, so dass das Eskalationsrisiko gering bleibt. Grundsätzlich gilt: Je größer in einer Gesellschaft das Verwundbarkeitspotenzial für Cyberangriffe relativ zum Potenzial des Angreifenden ist, desto zurückhaltender sollte die angegriffene Regierung sein, die Attacke zu erwidern. Die Folge einer relativ höheren Verwundbarkeit wäre dann eine Neigung zur Zurückhaltung, die besonders intensive Cyberkonflikte so lange unwahrscheinlich macht, wie diese Verwundbarkeit der meisten digitalisierten Gesellschaften wächst oder stabil hoch bleibt.

Die bundesdeutsche Debatte über den sogenannten Hack-Back, also gezielte Cybergegenschläge nach erfolgtem Angriff, spiegelt diesen Entwicklungstrend zumindest teilweise wider: Sollten Einheiten der Bundeswehr künftig nach Cyberangriffen auf deutsche Ziele mit digitalen Gegenschlägen antworten dürfen – und falls ja: Wie wäre deren Verhältnismäßigkeit sichergestellt? Die Debatte reicht aber auch über die Spezifika des Cyberraumes hinaus – denn käme es zu einer Legalisierung des sogenannten Hack-Back, dann müsste der Bundestag – im Sinne der dominanten Lehre der Parlamentarisierung des Streitkräfteeinsatzes – diese Einsätze in Art, Umfang, Ziel etc. mandatieren und wäre dabei an Artikel 87a des Grundgesetzes gebunden, welcher den Einsatz der Bundeswehr ausschließlich zur Landes- und Bündnisverteidigung oder im Rahmen kollektiver Zwangsmaßnahmen zulässt.

Field of Focus 4: Selbstregulation und Regulation
Im Rahmen der Exzellenzinitiative des Bundes und der Länder hat die Universität Heidelberg einen Großteil ihrer Forschung und Lehre unter dem Dach der großen Forschungsfelder themenbezogen zusammengeführt. Mit diesen vier „Fields of Focus“ (FoF) nutzt sie ihr Potenzial, durch Zusammenarbeit über die Grenzen der Disziplinen hinweg komplexe und für die Gestaltung von Zukunft zentrale Problemstellungen kompetent zu bearbeiten und damit gesellschaftliche Verantwortung zu übernehmen. FoF1 behandelt „Molekulare Grundlagen des Lebens, von Gesundheit und Krankheit“, FoF2 „Muster und Strukturen in Mathematik, Daten und in der materiellen Welt“, FoF3 „Kulturelle Dynamiken in globalisierten Welten“ und FoF4 „Selbstregulation und Regulation: Individuen und Gesellschaften“. Das zentrale Anliegen von FoF4 besteht darin, menschliche (Selbst-)Regulationsprozesse auf der Ebene von Individuen und Organisationen im interdisziplinären Dialog besser zu verstehen. An dieser Arbeit sind insbesondere Fächer der Fakultät für Verhaltens- und Empirische Kulturwissenschaften, der Fakultät für Wirtschafts- und Sozialwissenschaften sowie der Juristischen Fakultät beteiligt, daneben auch interdisziplinäre Forschungsverbünde, Forschungsstellen sowie außeruniversitäre Partner.

www.uni-heidelberg.de/de/forschung/forschungsprofil

Erste empirische Befunde

Unsere ersten empirischen Befunde zeichnen folgendes Bild: Autokratien nutzen regelmäßig nichtstaatliche Proxys, um Attribution zu erschweren. Dabei rangieren Russland, Iran, Nordkorea und China ganz oben auf der Liste. Sie verwenden aber unterschiedliche Proxytypen für unterschiedliche Zwecke: Russland nutzt nichtstaatliche Hackergrupppen mit Namen wie „Fancy Bear“, „Cozy Bear“, „Turla“ oder „Sandworm“ vorrangig, um mit disruptiven, das heißt zerstörerischen Angriffen oder Desinformationskampagnen (in Abgrenzung zur Cyberspionage) den gesellschaftlichen Zusammenhalt westlicher Demokratien zu unterminieren oder in konventionellen Konflikten, wie in der Ukraine, militärische Kontrahenten zu schwächen. Anders die Regierung Chinas: Die Volksrepublik nutzt für Hackerangriffe bislang oft spezialisierte Einheiten des

THE BLAME GAME IN CYBERSPACE

INFORMATION TECHNOLOGY AS A WEAPON?

SEBASTIAN HARNISCH & KERSTIN ZETTL

Academic and policy debates on the attribution of cyberattacks have yet to fully grasp the political dimension of this task. This article sets out some of the technical problems of identifying a perpetrator in cyberconflicts, but focuses mainly on the political dynamics of evading responsibility, and thereby blame, for cyberattacks. We have found that democratic and autocratic governments differ substantially in their conflict behaviour, for instance in their use of proxies.

Autocratic governments tend to use proxies to carry out offensive attacks on democratic states, whereas democratic governments, when attacked, try to avoid the costs of assigning political responsibility by having proxies attribute technical responsibility to an attacker. It follows that in democracies, the task of attributing cyberattacks to a perpetrator increasingly falls to private IT companies, a fact that could potentially undermine the principles of transparent and responsible government. Comparing autocratic systems, we also found that Russia uses non-state proxies for disruptive attacks in conventional conflicts, such as Ukraine, and to undermine the credibility of democratic institutions. In contrast, China uses state agencies mainly for cyber espionage to leapfrog military and economic competitors, in particular the United States.

Overall, our research suggests the utility of applying a comparative approach to informing the societal debate on cyberconflict and democratic governance: First, citizens should be aware that their governments are hesitant to name perpetrators because doing so might hurt their voters more than blurring responsibility. Second, stricter rules that obligate societal actors, such as companies, universities etc. to report attacks would help democratic societies to acknowledge their vulnerability and adress it accordingly. Third, civil society may play a crucial role in pushing governments to strengthen international norm-building processes so as to prevent cyberconflict escalation in the first place. ●

PROF. DR SEBASTIAN HARNISCH has held the Chair of International Relations and Foreign Policy at Heidelberg University's Institute for Political Science since 2007. In the past, he worked at universities in Trier, Munich, Beijing (China), New York (USA), Seoul (South Korea) and Tokyo (Japan). His research projects and publications deal with comparative foreign and security policy, theories of international relations, non-proliferation, internet politics and climate change. Another research focus is the attribution of cyberattacks, a subject he has been investigating since 2019 within the framework of a research project funded by the German Foundation for Peace Research.

Contact: sebastian.harnisch@ipw.uni-heidelberg.de

KERSTIN ZETTL (M.A.) is a research assistant and in 2019 joined a project on cyberconflicts that is funded by the German Foundation for Peace Research and headed by Sebastian Harnisch at Heidelberg University's Institute for Political Science. She is currently working on her doctoral thesis, a comparison of autocratic and democratic cyber proxy strategies. She studied political science, psychology and educational science at Heidelberg University.

Contact: kerstin.zettl@ipw.uni-heidelberg.de

"A clear definition of red lines in the digital space, and of the sanctions that apply when these lines are crossed, is the only way of limiting cyberconflicts and ensuring cybersecurity for a maximum number of users."

Ministeriums für Staatssicherheit oder der Volksbefreiungsarmee, um mit dem Diebstahl geistigen Eigentums einen kommerziellen, politischen oder militärischen Vorteil zu erlangen. Die Neigung zur Cyberspionage kann dabei auch patriotische nichtstaatliche Hackergruppen miteinbeziehen, die gegnerische Regierungsnetzwerke oder kritische gesellschaftliche Akteure angreifen, beispielsweise im Konflikt über die rivalisierenden Territorialansprüche im Südchinesischen Meer. Im Falle Nordkoreas haben wir festgestellt, dass sich der Angriffsschwerpunkt über die Zeit deutlich verschob: Vor 2014 richteten sich die Attacken nordkoreanischer Proxys, zumeist stationiert in China und Indien, auf politische und militärische Einrichtungen im Rahmen des Systemwettbewerbs gegen Südkorea und die USA. Seither dienen die Angriffe spezialisierter nordkoreanischer Cybereinheiten vornehmlich der Cyberspionage und dem finanziellen Diebstahl zum Zwecke des Regimeerhalts.

Vergleicht man nun diese Befunde für Autokratien mit jenen für demokratische Regime, so ergibt sich folgendes Bild: Bis 2016 lässt sich nur eine geringe Anzahl offizieller Attributionen von Cyberangriffen durch demokratische Regierungen finden. Zudem nahmen IT-Firmen über den Zeitraum seit 2000 eine immer bedeutsamere Rolle im (technischen) Zuschreibungsprozess ein. Dabei attribuieren sie nicht nur immer häufiger und ausführlicher im Rahmen ihrer technischen Berichte, sondern sie unterstützen auch vermehrt demokratische Regierungen im Falle offiziell erfolgter politischer Verantwortungszuweisungen, wie beispielsweise im Fall des erwähnten „DNC-Hacks“ bei den US-Demokraten.

Mit dem Amtsantritt von Donald Trump hat sich die zurückhaltende Attributionspraxis indes stark verändert: Seit 2017 macht die US-Regierung häufiger direkt ein feindliches Regime für Cyberangriffe verantwortlich. Ob dieser Befund Bestand haben wird, das wird sich zeigen. Gleichzeitig deuten sich aber auch Veränderungen der US-Regierungspraxis in einem anderen Cybersicherheitsbereich an: der Hortung von Cyberschadsoftware, vor allem sogenannter „zero-day-exploits“. Dies sind Softwaresicherheitslücken, die ungehindert ausgenutzt werden können, da sie dem Softwarehersteller bislang noch nicht bekannt waren und daher auch noch nicht geschlossen werden konnten. So hat im Januar 2020 die National Security Agency (NSA), die selbst zuvor eine große Sammlung von Schadsoftware „erworben“ hatte, die dann von nordkoreanischen Hackern gestohlen und verwendet worden war, den US-Softwaregiganten Microsoft auf einen schadhaften Code aufmerksam gemacht, anstatt diese Angriffsmöglichkeiten selbst zu nutzen.

Politische und gesellschaftliche Implikationen

Die Attribution von Cyberangriffen ist also eine soziale Zuschreibung, die alles andere als trivial ist. Unsere empirischen Ergebnisse zeigen, dass diese, je nach politischem Kontext, unterschiedlich erfolgt. Private Akteure mit eigenen kommerziellen, kriminellen oder ideellen Interessen ändern und prägen dabei die Deutungshoheit politischer Entscheidungsträger mit. Demokratische Regierungen können von der Funktionsübernahme des Privatsektors bei der Attribution profitieren. Tun sie es im Übermaß, so laufen sie Gefahr, ihrem eigentlichen Auftrag zuwiderzuhandeln, transparent und vor allem langfristig verantwortlich zu regieren.

Aus unserer Perspektive folgt hieraus dreierlei für die betroffenen demokratischen Gesellschaften: Erstens sollte ein hinreichendes Maß an politischer Transparenz im Zusammenhang mit der Attribution von Cyberattacken erreicht werden. Indem eine Regierung offen kommuniziert, warum sie in einem konkreten Fall einen bestimmten Täter oder Drahtzieher vermutet oder aber aufgrund technischer Widrigkeiten gar keine Attribution zu treffen vermag, kann sie die Legitimität ihres (Nicht-)Handelns wahren, ohne die Regierten bewusst im Unklaren zu lassen. Im Umkehrschluss: Je informierter eine Gesellschaft über die jeweilige Gefährdungslage im Netz ist, desto eher kann sie das notwendige Problembewusstsein entwickeln, um ihren Teil zum Schutz der digitalen Ziele beizutragen (Stichwort „Cyberhygiene“). Zweitens sollten demokratische Regierungen private Akteure, insbesondere Software- und Cybersicherheitsfirmen, stärker in die Pflicht nehmen, ihre Produkte umfassender gegen Manipulationen zu schützen sowie auch langfristig Softwareaktualisierungen für unterschiedlichste Endgeräte bereitzuhalten. Dies gilt vor allem für den Bereich der kritischen Infrastrukturen, denn in industriellen Anlagen im Bereich der Strom- oder Wasserversorgung werden oftmals veraltete Softwareversionen benutzt, weil die fortwährende Funktionserfüllung ein regelmäßiges Softwareupdate erschwert. Drittens sollten zivilgesellschaftliche Initiativen weiterhin die Normentwicklungsprozesse im Bereich der Cybersicherheit kritisch begleiten, um den nötigen öffentlichen Druck auf die nationalen Regierungen auszuüben. Denn nur wenn eindeutig definiert wird, welche roten Linien im digitalen Raum existieren und (in)wie(fern) deren Überschreiten sanktioniert werden kann und soll, lassen sich Cyberkonflikte begrenzen und Cybersicherheit für möglichst viele Anwender erreichen. ●