Am Anfang war die Attribution… Cyber-Angriffe und deren Beantwortung als Herausforderung demokratischen Regierens

Prof. Dr. Sebastian Harnisch, Institut für Politische Wissenschaft
Kerstin Zettl, M.A., Institut für Politische Wissenschaft

Als im US-Präsidentschaftswahlkampf 2016 der Öffentlichkeit nach und nach für die demokratische Partei kompromittierende Emailinhalte zugespielt wurden, lag die Zuschreibung (oder auch Attribution) einer Wahlbeeinflussung durch Russland auf der Hand. Private IT-Firmen und ungenannte Regierungsquellen deuteten mit dem Finger in Richtung des Kremls. Die russische Regierung, so der Vorwurf, hatte zwei Hackergruppierungen (sog. „Proxies“: staatlich beauftragte oder unterstützte nichtstaatliche Akteure) mit der Infiltrierung der Netzwerke des „Democratic National Committee“ (DNC) beauftragt. Was nicht folgte, war eine zeitnahe offizielle Zuschreibung der US-Regierung. 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. Unsere Daten zeigen, dass demokratische Regierungen regelmäßig davor zurückschrecken, bekannt gewordene Cyber-Angriffe auf ihr Land öffentlich bestimmten Tätern zu zuschreiben. Geschieht dies doch, werden bislang sehr selten fremde Regierungen direkt als Angreifer genannt und stattdessen von „staatlich-gesponserten“ Cyber-Angriffen gesprochen.

Der Heidelberger Cyberkonfliktdatensatz HD-CY.CON

Im einem von der Deutschen Stiftung Friedensforschung geförderten Projekt untersuchen wir ob und inwiefern sich Autokratien und Demokratien im Cyberkonfliktverhalten, insbesondere dem Gebrauch von Proxies unterscheiden. Aufbauend auf Untersuchungen die durch das Field of Focus-4 gefördert wurden, starten wir mit der These, dass Autokratien Proxies für Cyber-Angriffe nutzen, während Demokratien diese zur Attribution einsetzen. Hierbei wird der Akt der Zuschreibung an IT-Firmen ausgelagert und somit vermieden, dass eine demokratische Regierung durch die selbst getätigte Verantwortungszuweisung unter öffentlichen Handlungsdruck gerät. Wo kein Richter, da kein Täter. Für den Cyber-Space kann somit zudem gelten: Wo kein Täter, da keine notwendige Strafverfolgung.

Im Rahmen des Projektes „Sicherheit durch Verschleierung: Warum Regierungen Proxies in Cyberkonflikten einsetzen“ erstellen wir einen weltweit einmaligen Datensatz (HD-CY.CON). Dieser erfasst sowohl die beschriebene offensive Proxy-Nutzung autokratischer Staaten, sowie die vermutete defensive, auf Attribution ausgerichtete Proxy-Nutzung 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 werden für die Jahre 2000 bis 2017 Anzahl, Art und Attribution von Cyber-Angriffen und Gegenangriffen in ihrer Dynamik erfasst und analysiert.

Attribution ist der Anfang von Allem

Theoretisch folgen wir mit den beschriebenen Überlegungen den bisherigen Forschungsarbeiten zum sog. „Attributionsproblem“: In der Cybersicherheitsforschung wird darunter jene stark erschwerte Verantwortungszuweisung im Falle von Cyber-Attacken

verstanden, die auf die technische Komplexität und politische Verschleierungsmöglichkeiten im Internet zurückgeht. Ohne Attribution ist jedoch auch kein zielgerichtetes Handeln, bspw. Abschreckung durch glaubwürdige Androhung von Gegengewalt, möglich. Politische Verschleierungsstrategien dienen dazu, je nach Regimetypus, die Konsequenzen eigener, fremder oder beauftragter Handlungen zu vermeiden. So können konventionell unterlegene Autokratien durch die Beauftragung von Proxies diese dazu nutzen, die Kosten von Gegenmaßnahmen entweder auf die Beauftragten abzuwälzen oder gänzlich zu vermeiden. Demokratien dagegen können als Opfer von Angriffen die Verantwortungszuschreibung IT-Firmen überlassen und somit gesellschaftliche Forderungen nach Gegenmaßnahmen abwehren. Aufgrund ihrer großen digitalen Angriffsflächen scheuen demokratische Staaten längerfristige Cyberkonflikte, welche durch eigene Gegenmaßnahmen erst ausgelöst werden können. Zwar haben auch demokratische Regierungen nach Cybre-Angriffen ein starkes Interesse an politischer Verantwortungszuweisung. Doch sind sie im Falle einer offiziellen Zuschreibung durch gesellschaftlichen Druck eher gezwungen eine Reaktion folgen zu lassen: Und diese muss, aufgrund ihrer rechtsstaatlichen Standards, durch transparente und substanzielle technische Beweise unterfüttert werden können. Zudem besteht kein Konsens darüber, wie allgemein gültige Attributionsstandards zwischen Staaten aussehen sollten, wer über deren Einhaltung befindet und welche Form der Reaktion auf welche Art von Cyber-Angriff völkerrechtlich angemessen ist. Schon allein die Regeln für notwendige Cyberschutzmaß-nahmen und die Meldepflicht von Attacken auf Wirtschaftsunternehmen, darunter auch kritische Infrastruktur, sorgen für Kopfzerbrechen: So herrscht Streit darüber, wer die Kosten von Cyber-Angriffen tragen sollte: Der Staat oder die Unternehmen. Kurz: es bestehen substantielle Anreize für demokratische Regierungen, offizielle Zuschreibungen von Cyber-Angriffen zu vermeiden.

Attribution und Cyber-Forensik

In seiner Entstehungsgeschichte zielte das Internet als „Netzwerk der Netzwerke“ auf die ungehinderte Kommunikation von gleich(gesinnt)en Teilnehmern und weniger die zweifelsfreie Identifizierung der Kommunikationsteilnehmer. Dies beflügelte in der Gründergeneration u.a. die Vision von einem dezentralen, von staatlicher (All-)Macht losge-lösten und deshalb demokratisierenden Medium. Für potenzielle Angreifer bietet der technische Aufbau des Netzes – u.a. auch durch das sogenannte „Darknet“ - vielfältige Möglichkeiten der eigenen Identitätsverschleierung. Drei Wege sind besonders prominent: immer ausgefeiltere Verschlüsselungstechniken, die Verwendung von Proxy-Servern zum Umleiten des mit dem Angriff verbundenen Datentransfers über Transitländer, sowie die Instrumentalisierung von Botnetzen (aus mehreren gekaperten Computern zusammengesetztes Angriffsnetz, das für Angriffe instrumentalisiert werden kann).

Potenzielle Angreifer können daher relativ leicht sicherstellen, dass ihre Angriffe unerkannt bleiben, wenn sie dies wünschen. Dies gilt vor allem bei Cyberspionageattacken, denn der Angreifer zieht keinen Nutzen aus dem Bekanntwerden des Angriffes oder seiner Vorgehensweise (Detektion), sondern möchte die bestehenden Hintertüren auch für künftige Angriffe offen halten. Bei Cyberkonflikten mit kinetischen Effekten jedoch, bspw. der Abschaltung eines Stromkraftwerks auf fremden Territorium im Zuge eines konventionellen Krieges (Ukraine), ist das Ziel oft nicht nur die sichtbare Wirkung, sondern auch das Bekanntwerden der Angriffsart: der militärische Gegner soll verunsichert (Abschreckung von weiteren Eskalationshandlungen) oder dessen Bevölkerung 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 Drohpotential zu erkennen geben.

Zur eigenen Identitätsverschleierung sind sogenannte „False-Flag“-Attacken oft das Mittel der Wahl: Die Verwendung von Malware (schädigender Software), die in der Vergangenheit überwiegend einem bestimmten, anderen Cyber-Angreifer zugeordnet wurde, lenkt den Verdacht auf diesen und nicht 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, (die) Täter zu präsentieren und für ihr Handeln zu bestrafen. Aus einer inhaltlich falschen Attribution kann im schlimmsten Falle eine unintendierte Konfliktpotenzierung resultieren. Die ursprüngliche Konfliktpartei kann ungestört weiter agieren, während die neue ihrerseits genötigt wird, auf den „Vergeltungsangriff“ zu reagieren und damit möglicherweise einen neuen Konfliktzyklus in Gang setzt. Ein Überschwappen des Konfliktes in die „reale physische Welt“ kann hierbei nicht ausgeschlossen werden, wenn sich eine der Konfliktparteien besser gewappnet fühlt, den Konflikt in dieser Welt fortzuführen (sog. Spill-over-Effekt).

Die Rolle privater IT-Firmen

Unser Projekt geht insbesondere der Frage nach, ob, wann, und zu welchem Zweck Regierungen Proxies 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 in der Folge von Staaten, deren Proxies oder auch autonom agierenden nichtstaatlichen Akteuren, wie dem Hackerkollektiv Anonymous, auf Sicherheitslücken hin überprüft werden. War die Suche erfolgreich, so kann der jeweilige Angreifer dieses schadhafte Codesegment in einer Attacke einsetzen. Entsprechende Märkte hierfür versprechen (je nach „Güte der Malware“) erhebliche Gewinne für solche mit unterschiedlicher Reichweite und Wirkungsgrad. Gleiches gilt indes auch für die Entwicklung von Schutzlösungen – u.a. sog. Patches – welche die Schadsoftware oder deren Wirkung neutralisieren. Kann ein Anbieter oder Softwareentwickler nun auf beiden Märkten Angebote unterbreiten, profitiert er gleichsam zweimal: von der Entwicklung des Schwertes *und* des entsprechenden Schildes. Eine Verlockung, die dazu führen könnte, dass die Märkte für Schad- und Schutzsoftware exponentiell wachsen, während Gesellschaften immer mehr Alltagsobjekte (sog. Internet of Things, IOT) als potentielle Angriffsflächen einspeisen.

Entscheidungen unter Unsicherheit und Normwandel in der Cyberabwehrdebatte?

Politische Entscheider sind als attribuierende Akteure auf möglichst vollständige Informationen angewiesen. Aufgrund der strukturellen Ungewissheiten im Cyberraum arbeiten sie indes häufig nach dem Prinzip der hinreichenden Information. Im Falle von politischen Zuschreibungen in Cyberkonflikten führt dies zu zwei Entwicklungsszenarien: Insbesondere demokratische Entscheider versuchen aufgrund der Attributionsproblematik sowie damit verbundenen Eskalationsrisiken 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 also zusätzlicher Regeln, bspw. besonderer Meldepflichten, um das reale Ausmaß von Cyber-Angriffen besser zu erfassen. Im zweiten Szenario attribuieren Entscheider nur in solchen Fällen, wo die Eskalationsrisiken und damit die potentiellen

Reputationsverluste gering sind, d.h. bei niedrigschwelligen Cyber-Angriffen. 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 der Zuschreibung aber nicht zwingend eine konkrete Erwiderung, ein Gegenangriff, folgen, sodass das Eskalationsrisiko gering bleibt. Grundsätzlich gilt: je größer der anzugreifende Vektor einer Gesellschaft für Cyber-Angriffe relativ zum Angrifffsvektor des Angreifenden ist, desto zurückhaltender sollte die angegriffene Regierung sein, den Angriff zu erwidern. Die Folge einer relativ höheren Verwundbarkeit wäre dann eine Neigung zur Zurückhaltung, die besonders intensive Cyberkonflikte solange unwahrscheinlich macht, wie diese Verwundbarkeit der meisten digitalisierten Gesellschaften wächst oder stabil hoch bleibt.

Die bundesdeutsche Debatte über den sogenannten „Hack-Back“, also gezielte Cyber-Gegenschläge nach erfolgtem Angriff, spiegeln diesen Entwicklungstrend zumindest teilweise wider: Sollten Einheiten der Bundeswehr künftig nach Cyber-Angriffen 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 Cyberrraumes hinaus: Denn käme es zu einer Legalisierung des Hack-Back, dann müsste der Bundestag – im Sinne der dominanten Lehre der Parlamentisierung des Streitkräfteeinsatzes – diese Einsätze in Art, Umfang, Ziel etc. mandatieren und wäre dabei an Artikel 87a GG gebunden, welches den Einsatz der Bundeswehr ausschließlich zur Landes und Bündnisverteidigung zulässt.

Was die Empirie uns bisher verrät…

Unsere ersten empirischen Befunde zeichnen folgendes Bild: Autokratien nutzen regelmäßig nichtstaatliche Proxies 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“, um durch disruptive Angriffe oder Desinformationskampagnen den gesellschaftlichen Zusammenhalt westlicher Demokratien zu unterminieren oder militärische Kontrahenten in konventionellen Konflikten (Ukraine) zu schwächen. Anders die Regierung Chinas: der Volksrepublik dienen Hackerangriffe oft spezialisierter Einheiten des Ministeriums für Staatssicherheit oder der Volksbefreiuungsarmee, um durch den Diebstahl geistigen Eigentums einen kommerziellen, politischen oder militärischen Vorteil zu erlangen. Die Neigung zur Cyberspionage kann, wie bspw. im Konflikt über die rivalisierenden Territorialansprüche im Südchinesischen Meer, auch patriotische nichtstaatliche Hackergruppen mit einfassen, die gegnerische Regierungsnetzwerke oder kritische gesellschaftliche Akteure angreifen. Im Falle Nordkoreas verlagerte sich nach 2014 der Schwerpunkt der zuvor überwiegend aus dem Ausland (China und Indien) verübten, disruptiven Proxy-Cyber-Angriffe auf politische und militärische Einrichtungen in Südkorea und den USA zu Cyberspionage und finanziellem Diebstahl zum Zwecke des Regimeerhalts.

Im Vergleich stützen unsere Analysen auch die vorgestellten Überlegungen für das Verhalten demokratischer Staaten. 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 bspw. im Fall des erwähnten „DNC-Hacks“.

Mit dem Amtsantritt von Donal Trump hat sich die zurückhaltende Attributionspraxis anscheinend verändert: seit 2017 macht die US-Regierung häufiger direkt ein feindliches Regime für Cyber-Angriffe verantwortlich. Ob dies Bestand hat, wird sich zeigen. Gleichzeitig deuten sich Veränderungen der US-Regierungspraxis in einem anderem Cybersicherheits-bereich, der Hortung von Cyberschadsoftware, vor allem sog. „zero-day-exploits“, an. So hat jüngst die National Security Agency (NSA), der zuvor eine große Sammlung von Schadsoftware selbst gestohlen und von nordkoreanischen Hackern verwendet worden war, den US-Softwaregiganten Microsoft auf einen schadhaften Code aufmerksam gemacht, anstatt diese Angriffsmöglichkeiten selbst zu nutzen.

Politische und gesellschaftliche Implikationen

Attribution von Cyber-Angriffen ist also eine soziale Zuschreibung, die alles andere als banal 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 von politischer Entscheidungsträger. Demokratische Regierungen können von der Funktionsübernahme des Privatsektors profitieren. Tun sie es, so laufen sie jedoch Gefahr, ihrem Auftrag, transparent und vor allem langfristig verantwortlich zu regieren, zuwider zu handeln.

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 Cyber-Attacken erreicht werden. Denn je informierter eine Gesellschaft über die jeweilige Gefährdungslage im Netz ist, desto eher kann sie auch das notwendige Problembewusstsein entwickeln, um ihren Teil zum Schutz der digitalen Ziele beizutragen (Stichwort „Cyber-Hygiene“). Zweitens sollten demokratische Regierungen private Akteure, u.a. Software- und Cybersicherheitsfirmen, stärker in die Pflicht nehmen, ihre Produkte umfassender gegen Manipulationen zu schützen, sowie auch langfristig Softwareaktualisierungen für unterschiedlichste Endgeräte bereitzuhalten, inbesondere für den Bereich der kritischen Infrastrukturen. Hier werden oftmals veraltete Softwareversionen genutzt, weil die fortwährende Funktionserfüllung ein regelmäßiges Softwareupdate erschwert. Drittens sollten zivilgesellschaftliche Initiativen weiterhin die Normentwicklungsprozesse im Bereich des Cybersicherheit kritisch begleiten, um ggf. den nötigen Druck auf die nationalen Regierungen auszuüben. Denn nur wenn eindeutig definiert wird, welche rote 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.