Cyberspace wird zum politischen Schlachtfeld

Erstmals bezichtigen die USA Russland offiziell des staatlichen Hackings

Politisch motivierte Angriffe gegen einzelne Personen und ganze Staaten häufen sich im virtuellen Raum. Wer die Hacker sind, ist aber schwer nachzuweisen.

VON MYRIAM DUNN CAVELTY

Kriege werden unter anderem auch mit dem Laptop geführt. GAETAN BALLY / KEYSTONE

Nachdem mehrere Monate in den Medien bloss darüber spekuliert worden war, hat Washington Anfang Oktober Moskau offiziell bezichtigt, die amerikanischen Wahlen mithilfe von Hackerangriffen auf verschiedene politische Ziele beeinflussen zu wollen. In der Erklärung heisst es, die Nachrichtendienste der USA seien aufgrund der Vorgehensweise und des Ausmasses der Angriffe überzeugt, dass «nur Russlands höchstrangige Regierungsverantwortliche diese Aktivitäten genehmigt haben können». Es handle sich bei den Cyberattacken seit dem Sommer um Methoden, die für Russland nicht neu seien.

Putins Troll-Armee

Da die Beziehungen zwischen Russland und Amerika allgemein gespannt sind, erstaunt es nicht, dass Washington insbesondere nach steigendem innenpolitischem Druck bereit ist, Russland offiziell für die Hackerangriffe verantwortlich zu machen. Noch weniger erstaunt der Entscheid, wenn man diese Kampfansage als Trend im Kontext der Cyber-Kriegsführung versteht.

Es ist kein neues Phänomen, dass politische Akteure versuchen, die öffentliche Meinung zu manipulieren. Was sich jedoch verändert hat, ist das mediale Umfeld. Webbasierte Dienste und Inhalte sowie die clevere Nutzung von sozialen Netzwerken und den damit verbundenen Algorithmen eröffnen staatlichen und nichtstaatlichen Akteuren neue Möglichkeiten des länderübergreifenden «Media Hacking». Die gezielte Manipulation von Inhalten im Internet ist eine Taktik, die Moskau schon seit Jahren systematisch einsetzt. Spätestens seit dem Ukraine-Konflikt ist bekannt, dass sich Russland einer «Troll-Armee» – auch Kremlbots oder Web-Brigaden genannt – bedient. Im Internet wird als Troll bezeichnet, wer Kommunikation unter anderen Benutzern durch provokante, beleidigende oder destruktive Art stört oder mit Absicht in falsche Richtungen lenkt. Ziel der russischen Trolle ist es, durch koordiniertes und kollektives Auftreten die Meinung auf nationalen und vermehrt auch internationalen Websites zu beeinflussen.

Eine neuere Dimension ist dabei das Eindringen in Computersysteme, um politische Gegner mit den so gewonnenen privaten und persönlichen Informationen zu diskreditieren oder zu erpressen. Im Laufe des Sommers ist sogar der amerikanische Nachrichtendienst National Security Agency (NSA) Opfer eines Hackerangriffs geworden, der laut gewissen Experten auf Russland zurückgehen könnte. Im Nachgang wurde im Internet geheime Software veröffentlicht, die die NSA für die Cyberspionage entwickelt hat. Die Kombination von Datendiebstahl und Beeinflussung entspricht durchaus der russischen Vorstellung von «Informationskrieg». Im Gegensatz zu der euroatlantischen Sichtweise, die den Cyberkrieg eng als zerstörerische Attacken auf Computersysteme und kritische Infrastrukturen definiert, geht Russland das Thema ganzheitlicher an: Neben Informationssystemen sind der Mensch und seine Meinung das wichtigste Ziel seiner Informationskriege.

Aber wie kann man mit Sicherheit wissen, dass Russland dahintersteckt? Die Schwierigkeit, Cyberangriffe mit ausreichender Sicherheit einem Ursprung beziehungsweise einem Täter zuzuordnen, wird als Attributionsproblematik bezeichnet. Die Spurensicherung und somit die eindeutige Zuordnung eines Angriffs sind meist sehr schwierig, langwierig und manchmal sogar unmöglich: Erstens werden Datenpakete im Internet getrennt und über verschiedene Routen und Server in den unterschiedlichsten Ländern verschickt. Zweitens gibt es viele Möglichkeiten, Spuren zu verwischen oder falsche zu legen, etwa im Quellcode einer Schadsoftware: Dieser kann Hinweise auf den Ursprung einer Schadsoftware liefern, aber natürlich auch mit Absicht auf eine falsche Fährte locken. Insbesondere für die Strafverfolgung, die auf gerichtsfeste Beweise angewiesen ist, heisst das, dass eine Bestrafung oft ausbleiben muss.

Auch in der internationalen Politik wird die Attributionsproblematik seit langem als grosses Problem beschworen, da sie aufgrund der «glaubhaften Abstreitbarkeit» Tür und Tor für den Missbrauch des Internets zu politisch-strategischen Zwecken öffne. Interessanterweise ist es in der Realität aber so, dass seit Jahren, zumindest auf informeller Ebene, durchaus Schuldzuweisungen für Cyberangriffe gemacht werden. Diese beruhen nie auf technisch eindeutigen Beweisen, sondern bedienen sich der «Cui bono»-Logik («Wem zum Vorteil?») – ein Prinzip, das den Schuldigen in demjenigen vermutet, der am meisten von einer Tat profitiert. Eine Attribution erfolgt dann über Indizienbeweise, wie es auch bei den derzeitigen Russland-Hacks der Fall zu sein scheint.

Ein neuer Trend ist, dass die USA vermehrt bereit sind, diese Schuldzuweisungen offiziell auszusprechen und Konsequenzen anzudrohen. Diese Bereitschaft ist Teil des Bestrebens, die Wirkung von «Abschreckung» im virtuellen Raum zu stärken. Abschreckungsstrategien spielten vor allem während des Kalten Kriegs eine zentrale Rolle, um die Wahrscheinlichkeit eines (nuklearen) Angriffs zu reduzieren.

Abschreckung als Strategie

Da Abschreckung unter anderem über die Angst vor Strafe operiert, kann sie im Cyberspace nur funktionieren, wenn glaubhaft gemacht werden kann, dass Attribution möglich ist – und dass der Wille da ist, zu bestrafen. Welche technischen und geheimdienstlichen Kapazitäten die USA im Bereich der technischen Attribution heute schon haben, wird bewusst im Vagen gelassen; es wird aber gerne suggeriert, dass eindeutige Zuordnungen möglich seien.

Dieser Logik folgend ist zu erwarten, dass in Zukunft weiterhin klare Schuldzuweisungen erfolgen werden – und es dabei meist unklar bleiben wird, wie viel die amerikanische Regierung wirklich weiss und ob es wirklich der bezichtigte Gegner war – insbesondere, da Dementi der Gegenseite immer auf dem Fuss folgen. Ob das blosse Androhen von Konsequenzen reicht oder ob tatsächlich Taten folgen müssen, wird sich weisen. Die in der Politik öffentlich diskutierten Bestrafungen reichen je nach Schwere des Vorfalls von Sanktionen über Vergeltungsaktionen im Cyberspace bis hin zu einem unter internationalem Völkerrecht legitimierten kinetischen Gegenschlag.

Konkret hat Washington im März dieses Jahres iranische Hacker angeklagt, die im Auftrag ihrer Regierung amerikanische Infrastruktur angegriffen haben sollen. 2014 waren es fünf Angehörige des chinesischen Militärs, die wegen Internetangriffen und Wirtschaftsspionage angeklagt wurden. Neben solchen eher symbolischen Aktionen ist es am wahrscheinlichsten, dass die USA bei wirklich unangenehmen Vorfällen so lange wie möglich auf verdeckte Gegenschläge im Bereich der Netzwerkoperationen setzen werden, um den Konflikt nicht eskalieren zu lassen und gleichzeitig Stärke im virtuellen Raum zu demonstrieren. Solche Gegenschläge als «Revanche» hat der amerikanische Vizepräsident Joe Biden auch jüngst im Fernsehen angekündigt.

Bleibt vielleicht die Frage, ob Russland die Wahlen mit seinen bisherigen Methoden überhaupt beeinflusst hat. Es scheint so, als ob die Angriffe neben beträchtlichem Wirbel nur dazu geführt haben, dass die Parteivorsitzende der Demokraten zurückgetreten ist, ohne sichtbare Auswirkungen auf den Wahlkampf. Darüber, ob noch weitaus brisantere Informationen auf schlecht gesicherten Servern zu finden sein könnten, kann nur spekuliert werden – das Potenzial für weitere, auch richtungsweisende Skandale ist aber sicherlich ernst zu nehmen.

Was zudem mit Sicherheit gesagt werden kann, ist, dass politisch motiviertes Hacking, sei es von Russland initiiert oder nicht, auch in Zukunft ein fester Bestandteil von Wahlprozessen bleiben wird. Ob es dabei bei Diebstahl von heiklen Daten bleibt, ist fragwürdig. In diesem Zusammenhang lässt es aufhorchen, wenn in der offiziellen Erklärung Washingtons auch die Rede davon ist, dass von russischen Servern aus versucht worden sei, Zugriff auf elektronische Wahlsysteme zu erlangen – bisher vergeblich, wie betont wird.

Alles Säbelrasseln nützt nicht viel, wenn die Sicherheit von technischen Systemen, die in unserem Leben allgegenwärtig sind und viele zentrale Funktionen ausführen, vernachlässigt wird. Auch wenn ein hundertprozentiger Schutz der Informationsinfrastruktur nie möglich sein wird, so erhöht man doch auf diesem Weg die Kosten für den Gegner beträchtlich. Das ist ein weiterer wichtiger Aspekt der Abschreckung, vor allem im Bereich der Cyberkonflikte: dem Gegner das Erreichen seiner militärischen und politischen Ziele zu verwehren.

Dr. **Myriam Dunn Cavelty** ist stellvertretende Leiterin für Forschung und Lehre am Center for Security Studies der ETH Zürich.

Nicht einmal der Stolz auf 1956 vermag Ungarn zu einen

Geteiltes Gedenken der politischen Lager und ein Pfeifkonzert für Ministerpräsident Orban

MERET BAUMANN, WIEN

Vor zehn Jahren wurde der offizielle Festakt zum 50. Jahrestag des ungarischen Volksaufstands gegen die Sowjetmacht, an dem Staatsgäste aus über 50 Ländern teilnahmen, von schweren Krawallen überschattet. Die tiefe innenpolitische Krise nach dem Bekanntwerden der berühmt gewordenen «Lügenrede» des damaligen sozialistischen Regierungschefs Ferenc Gyurcsany hatte am Feiertag neuerliche Demonstrationen der konservativen Opposition zur Folge, die in Ausschreitungen mündeten, bei denen die Polizei Tränengas einsetzte. Beobachtern dienten die Ereignisse als weiterer Beweis für die tiefe Spaltung im Land; von einem «kalten Bürgerkrieg» war in dieser Zeitung die Rede. Zehn Jahre später hat der Gedenkanlass vom Sonntag gezeigt, dass der Graben nicht zugeschüttet ist.

Nicht einmal der für Ungarn so bedeutende Stolz auf den heldenhaften Freiheitskampf vermag die Nation für einen Tag zu einen. Die Parteien luden ihre Anhänger an unterschiedlichen Orten in Budapest zu Feierlichkeiten, während der Zugang zum Kossuth-Platz vor dem Parlament für den offiziellen Festakt streng kontrolliert wurde – offiziell aus Sicherheitsgründen, laut Regierungskritikern aber auch, um Unmutsbekundungen weitestgehend zu verhindern. Es nützte jedoch nichts. Bereits die Rede von Präsident Janos Ader wurde durch Protest gestört, ebenso jene des ausländischen Ehrengasts, des polnischen Staatschefs Andrzej Duda. Der ungarische Volksaufstand hatte einst aus Solidarität mit den Arbeiterprotesten im Sommer 1956 in Poznan sowie der Studentendemonstration vier Monate später in Warschau begonnen.

Zu einem gellenden Pfeifkonzert und lauten Buhrufen kam es, als Ministerpräsident Viktor Orban zu Tausenden seiner Anhänger auf dem Platz sprach. Einige Regierungskritiker hatten Zutritt zu dem Gelände erhalten, Hunderte weitere fanden sich entlang den Absperrungen ein und verschafften sich mit Trillerpfeifen Gehör. Laut Augenzeugen kam es auch zu kleineren Zusammenstössen mit Regierungsanhängern und der Polizei. Kritiker werfen Orban vor, mit der Machtanhäufung in den Händen seiner Partei Fidesz und der Hinwendung zu Moskau die Werte der Revolution von 1956 zu verraten. Als neuster Beweis dafür dient ihnen die Einstellung der linksliberalen Zeitung «Nepszabadsag» vor zwei Wochen. Nach einem Bericht des Portals 444.hu vom Sonntag soll das auflagenstärkste politische Blatt des Landes und eines der letzten Sprachrohre der Opposition unmittelbar vor dem Verkauf an das Unternehmen von Lörinc Meszaros stehen; dieser ist ein Vertrauter des Regierungschefs und Bürgermeister von dessen Heimatgemeinde Felcsut. Einige Demonstranten hielten Exemplare der Zeitung hoch, die zuletzt unrühmliche Affären zweier Mitstreiter Orbans enthüllt hatte.

AP

Viktor Orban
Regierungschef von Ungarn

Orban stellte sich und seine Regierung in seiner Rede in eine Linie mit den Helden von 1956. Alle dreissig Jahre schreibe Ungarn Geschichte, erklärte der Ministerpräsident. 1956 mit dem Aufstand, 1989 mit der Durchtrennung des Eisernen Vorhangs und 2016, indem man die Massenzuwanderung gestoppt habe. Selbst in hoffnungslosen Zeiten hätten die Ungarn ihre Freiheit nicht aufgegeben. Nun gelte es, die EU als Bündnis souveräner Staaten zu bewahren und die «Sowjetisierung» Brüssels zu stoppen. In einer zweifelhaften Interpretation des vor drei Wochen am Quorum gescheiterten Quoten-Referendums betonte er, die Ungarn hätten «neue Einigkeit» demonstriert. Die Feier zeigte erneut das Gegenteil.