Auf dem Weg zur Cyber-NATO

Zum Schutz unserer liberalen Demokratien im digitalen Zeitalter

Toomas Hendrik Ilves | **Die Digitalisierung bringt ungeahnte Vorteile, aber auch Gefahren für liberale Demokratien. Im digitalen Zeitalter hat geografische Distanz ihre Bedeutung verloren. Hinzu kommt, dass Cyber-Bedrohungen asymmetrisch sind. Liberale Demokratien können nicht mit denselben Mitteln zurückschlagen, mit denen sie angegriffen werden.**

Jeder ist bedroht. Ein einziges russisches Hacker-Kollektiv, die Sofacy Group oder auch „Fancy Bear" genannt, hat in den vergangenen Jahren die Server von Ministerien, Parteien und Politikern in den USA, Deutschland, den Niederlanden, Schweden, der Ukraine, Italien und Frankreich angegriffen. Ins Visier gerieten auch militärische Kommunikationssysteme und Computer des Weltleichtathletikverbands, der unter anderem gegen Doping vorgeht.

Dabei ist die Sofacy Group allein in Russland nur eines unter vielen Hacker-Kollektiven – und die russische Regierung auch nicht das einzige autoritäre Regime, das sich mithilfe von Cyber-Attacken politische Vorteile verschaffen will. Es ist offensichtlich, dass der Iran eigene Cyber-Angriffe ausführt. Chinesische Hacker, die sich im Dunstkreis der Streitkräfte bewegen, haben es schon seit Langem auf militärische Computersysteme und auf das geistige Eigentum ausländischer Firmen auf der ganzen Welt abgesehen.

Das digitale Zeitalter hat uns in eine Ära neuer Gefahren für unsere Sicherheit katapultiert, die wir uns vor zehn Jahren noch nicht hätten ausmalen können. Nationale Regierungen tun sich schwer damit, auf diese neuen Bedrohungen angemessen zu antworten. Multilaterale Organisationen wie die NATO und die EU sind sogar noch langsamer. Auch die Vereinten Nationen haben es nicht geschafft, ein Übereinkommen zum Verbot von digitalen Waffen zu vermitteln. Dazu braucht es – und dafür plädiere ich in diesem Aufsatz – eine „Cyber-NATO", eine Koalition liberaler Demokratien, die den heute allgegenwärtigen digitalen Gefahren entgegentreten kann. Das wird nicht leicht werden. Aber die Alternative ist schlimmer.

Der Cyber-Krieg hat begonnen

Cyber-Angriffe gibt es seit nunmehr fast 40 Jahren. In der Vergangenheit wurden sie jedoch vorrangig für Spionage genutzt und nicht, um Gegnern direkten

Bild nur in Printausgabe verfügbar

Schaden zuzufügen oder um politische Aussagen zu machen. Es ist erst zehn Jahre her, dass sich erstmals eine großangelegte Cyber-Attacke direkt gegen die Sicherheit eines Staates und seiner Bürgerinnen und Bürger wendete.

Jede Geschichte des Cyber-Krieges beginnt mit dem Angriff auf Estland im Jahr 2007, als die Server der estnischen Verwaltung, der Banken und Nachrichtensender mithilfe von so genannten Denial-of-Service-Attacken oder DDOS-Attacken lahmgelegt wurden. In der Folge wurden fast alle öffentlichen Online-Dienste für Bürgerinnen und Bürger blockiert. Natürlich gab es Cyber-Angriffe schon viel früher, doch diese Attacke unterschied sich von allen vorherigen: Sie erfolgte unverhohlen und vor den Augen der Öffentlichkeit. Sie fiel als „Fortsetzung der Politik mit anderen Mitteln" unter die Kriegsdefinition des berühmten Militärwissenschaftlers Carl von Clausewitz: Der Angriff war eine Reaktion auf die Entscheidung der estnischen Regierung, eine Statue aus der Sowjetzeit aus der Hauptstadt Tallinn zu entfernen.

Seit 2007 hat sich die offene Cyber-Kriegsführung als Fortsetzung der Politik mit anderen Mitteln ausgebreitet und immer bedrohlichere Formen angenommen. In Konfliktgebieten legen DDOS-Attacken im Vorfeld von Bombenangriffen ganze Landstriche lahm (Georgien, 2008); Stromnetze werden ausgeschaltet (Ukraine, 2016 und 2017); private Firmen werden angegriffen (Sony, 2015); Parlamente werden gehackt (Deutscher Bundestag, 2015 und 2016), Denkfabriken und politische Parteien (die National Committees der Demokraten und Republikaner in den USA, 2015/16), einzelne Politiker (Hillary Clinton, 2016; Emmanuel Macron, 2017) und Ministerien (Ministerien in den Niederlanden, das italienische Außenministerium sowie das State Department und das Verteidigungsministerium der USA) werden ins Visier genommen. Im Zuge eines besonders dreisten Angriffs stahlen Hacker die Personalakten von

23 Millionen Mitarbeitern der amerikanischen Verwaltung. Leaks und Zeugenaussagen aus den USA weisen auch daraufhin, dass eine ausländische Regierung im Vorfeld der US-Präsidentschaftswahlen versuchte, Wählerdaten in 21 (vielleicht sogar in bis zu 39 Bundesstaaten) zu modifizieren oder zu löschen.

Lahmlegen und zerstören

Vor einem Jahrzehnt existierten großangelegte elektronische Angriffe auf Staaten nur in der Theorie. So bezweifelte man in der NATO, ob 2007 ein solcher Angriff auf Estland wirklich stattgefunden habe. Doch seit man erkannt hat, dass es politisch motivierte DDOS-Attacken gibt und welche weitreichenden Folgen sie haben, hat sich der Fokus beim Thema Cyber-Sicherheit verändert. Mittlerweile spielen Experten alle möglichen Szenarien durch. Dabei geht es um die Nutzung von Malware, um kritische Infrastruktur lahmzulegen oder sogar zu zerstören; Strom- und Kommunikationsnetze, Wasserversorgungssysteme und sogar die Ampelschaltungen in größeren Städten. Attacken dieser Art sind keine DDOS-Angriffe mehr, die lediglich den Zugang blockieren, sondern erfordern „Hacks“, also Einbrüche in Server oder Computersysteme.

Der Begriff Cyber-Attacke umfasst viele Aktivitäten

Neuartige Cyber-Attacken können ganze Länder lahmlegen oder ihre Streitkräfte kampfuntauglich machen. Im Falle eines konventionellen Militärschlags wären sie dann wehrlos. Bereits 2010 schreckte uns der Stuxnet-Computerwurm auf, der die iranischen Plutonium-Zentrifugen außer Kontrolle brachte. Er machte deutlich, dass Cyber-Angriffe inzwischen fähig sind, physische Systeme ernsthaft zu beschädigen. Der ehemalige US-Verteidigungsminister Leon Panetta warnte bereits 2012 vor einem „virtuellen Pearl Harbor“.

Diese Beispiele verdeutlichen, dass der Begriff Cyber-Attacke eine Vielzahl von Aktivitäten umfasst, von der Zerstörung der kritischen Infrastruktur zu subtileren Angriffen: Hacks gegen Politiker, um kompromittierendes Material zu verbreiten und die Integrität von Wahlkämpfen zu gefährden.

Nationale und multilaterale Gegenstrategien

Nur langsam wird sich die Welt der Cyber-Bedrohungen bewusst. Obwohl die USA und andere Länder die potenziellen Gefahren schon in den frühen 1990er Jahren vorhersahen – damals waren bereits Hacker-Angriffe registriert worden –, hielten sie sich zurück. Wie bereits beschrieben, tat sich auch die NATO lange schwer, den Angriff auf Estland 2007 überhaupt erst als einen solchen zu erkennen. Es dauerte bis 2011, bis die Münchner Sicherheitskonferenz, das wichtigste Treffen westlicher Sicherheitspolitiker, eine Diskussion zum Thema Cyber-Sicherheit veranstaltete.

Bis zu diesem Zeitpunkt ging der Westen noch von einem Konzept symmetrischer Kriegsführung aus. Was auch immer Cyber-Angreifer einem antaten: Sobald man herausgefunden hatte, wer sie waren, würde man zurückschlagen können. Cyber-Attacken waren also eine neue Unterkategorie der konventionellen Kriegsführung. Die USA erklärten elektronische Angriffe 2010 zur fünften „Dimension“ der Kriegsführung (neben Land, See, Luft und Weltraum).

Obwohl die NATO die potenziellen Gefahren von Cyber-Attacken und digitaler Propaganda mittlerweile erkannt hat, hat die Allianz in der Praxis erschreckend wenig unternommen. Zwar gründete man das so genannte CCD COE, das Cooperative Cyber Defence Center of Excellence, im estnischen Tallinn und eröffnete später das „Center for Strategic Communication" in der lettischen Hauptstadt Riga. Doch insgesamt kooperieren die NATO-Bündnispartner auf dem Gebiet der Cyber-Sicherheit noch viel zu wenig.

Demokratie unter Beschuss

Propaganda, Falschnachrichten und Desinformation sind mindestens so alt wie das trojanische Pferd. Doch Desinformation, wie wir den Begriff bis ins späte 20. Jahrhundert verstanden, richtete keinen großen Schaden an. Ohne digitale Plattformen ließen sich Falschnachrichten nicht so schnell verbreiten, dass sie die traditionellen Medien übertönten. Auch Wählerverzeichnisse konnten nicht in großem Stil und über mehrere Bezirke hinweg manipuliert werden.

Es ist kaum mehr als ein Jahr her, dass sich unter Experten die Erkenntnis durchgesetzt hat, dass demokratische Wahlen beeinflusst werden. Zu den bisherigen Manipulationen zählte etwa das „Doxing", also die Weiterverbreitung gehackter Informationen, um Personen wie Hillary Clinton und Emmanuel Macron zu schaden. Derartige Strategien werden oft mit Falschmeldungen unterfüttert, die durch „bots" (Roboter-Accounts) in den sozialen Netzwerken weiterverbreitet werden. Sobald diese Fake News eine gewisse Reichweite erzielen, werden sie massenweise von echten Nutzerinnen und Nutzern geteilt. Eine US-Studie belegt, dass Internetnutzer in den drei Monaten vor den Präsidentschaftswahlen rund 8,7 Millionen Fake News aufriefen, aber nur 7,3 Millionen authentische Nachrichtenartikel.

Wahlmanipulation zugunsten von Wunschkandidaten

Falschnachrichten können auch benutzt werden, um die öffentliche Meinung zu beeinflussen. Der #Syriahoax, unter dem die Information verbreitet wurde, das syrische Regime habe im Frühjahr 2017 chemische Waffen eingesetzt, war ein Fake aus dem Westen und wurde mithilfe so genannter Twitterbots weiterverbreitet. Falschmeldungen über die Stationierung von NATO-Truppen in Osteuropa sind inzwischen ein Alltagsphänomen.

Aus sicherheitspolitischer Sicht ist digitale Manipulation für unsere Widersacher sehr attraktiv. Warum sollte man sich mit Militärinterventionen oder konventioneller Kriegsführung (oder sogar mit Cyber-Angriffen) abmühen, wenn es reicht, einem Kandidaten den Weg ins Amt zu ebnen, der für die eigenen Interessen nützlich ist? Ein Wahlsieg von Le Pen in Frankreich oder eine Abwahl von Angela Merkel in Deutschland hätten der europäischen Russland-Politik stärker geschadet als jedes militärische Manöver.

Autokratische Staaten müssen sich um Wahlbeeinflussung von außen keine Sorgen machen, weil diese so oder so von den Machthabern im eigenen Land manipuliert werden. Zugleich ist es fast unvorstellbar, dass eine liberale Demokratie gegen Russland dieselben Mittel anwenden würde, die Russland während der Wahlkämpfe gegen die USA und Frankreich einsetzte. Und selbst wenn man den Versuch wagen würde, wäre er zum Scheitern verurteilt.

Wahlmanipulationen können überhaupt nur dort Wirkung entfalten, wo faire und freie Wahlen stattfinden. Insofern ist die neue Bedrohung ihrer Natur nach asymmetrisch.

Die Nähe zu potenziellen Feinden war über Jahrhunderte und Jahrtausende hinweg ein prägender Faktor der Sicherheitspolitik. Staaten wurden üblicherweise von ihren direkten Nachbarn angegriffen, nicht von Ländern, die auf der anderen Seite der Erde lagen. Bis zur Erfindung der Interkontinentalrakete war die Distanz zum Feind der beste Schutz.

Heute dagegen sind wir für digitale Bedrohungen in gleichem Maße anfällig, egal ob wir Tür an Tür mit unserem Feind wohnen oder weit weg. Eine Konsequenz daraus ist, dass im 21. Jahrhundert das Fundament, auf dem viele der uns bekannten Allianzen – angefangen mit dem Peloponnesischen Bund – gegründet wurden, geschwächt wurde oder überhaupt nicht mehr existiert. Auch die NATO wird durch die Einsatzmöglichkeiten von Panzern, die Reichweite von Bombenflugzeugen und die Stationierung von Soldaten definiert. Liberale Demokratien mit freien und fairen Wahlen wie Japan, Australien und Uruguay können wegen ihrer geografischen Distanz vom Atlantik keine Mitglieder der NATO werden. Trotzdem ist die kritische Infrastruktur dieser Länder heute genauso verletzlich wie die von osteuropäischen Staaten. Ihre Wahlen und demokratischen Strukturen sind nicht weniger in Gefahr als die in den USA oder Deutschland. Digitale Bedrohungen kennen keine Entfernungen.

Digitale Bedrohungen kennen keine Entfernungen

Eine demokratische Allianz im digitalen Zeitalter

Angesichts dieser Entwicklungen müssen Demokratien anfangen, über ihren traditionellen Sicherheitsbegriff hinaus zu denken. Heute kann uns der Krieg unabhängig von der Reichweite von Flugzeugen und Raketen erreichen. Neben den bereits existierenden Verteidigungsbündnissen brauchen wir deswegen eine neue Allianz. Sie sollte sich nicht an der Geografie orientieren, sondern die Demokratien verteidigen, in denen freie und faire Wahlen stattfinden, in denen Rechtsstaatlichkeit herrscht und Grundrechte das Fundament der Gesellschaft bilden.

Diese Idee ist nicht neu. Schon bevor das digitale Zeitalter anbrach, schlugen Madeleine Albright und John McCain vor, einen Bund der Demokratien zu gründen. Ihre Vorschläge fanden damals nicht viel Anklang; sie waren auch nicht aus Sicherheitsgründen vorgebracht worden. Heutzutage allerdings ist jede Demokratie verwundbar, und wir werden uns dessen immer mehr bewusst. Die Aussichten, dass ein derartiges Sicherheitsbündnis zustande kommt, sind deswegen besser. Doch braucht es die Unterstützung der großen Länder innerhalb und außerhalb der NATO. Nur dann wird es gelingen, unsere liberalen Demokratien besser vor den Gefahren des 21. Jahrhunderts zu schützen.

Toomas Hendrik Ilves war von 2006 bis 2016 Staatspräsident von Estland. Heute ist er Distinguished Visiting Fellow an der Hoover Institution.