Cyberwar

Christian Stöcker | **Die Debatte über virtuelle Kriege pendelt häufig zwischen Hysterie und völliger Unterschätzung der Gefahren. Sind Hackerangriffe und massenhafter Datendiebstahl bereits Kriegsakte? Lassen sie sich einem Aggressor eindeutig zuordnen? Und wie gut ist gerade Deutschland gerüstet? Sechs Thesen auf dem Prüfstand.**

Der Cyberwar ist der Kalte Krieg von heute

Nur, wenn man „Kalter Krieg" sehr wörtlich definiert. Wenn also ein kalter Krieg einer ist, in dem nicht mit Bomben und Granaten, mit Schusswaffen und Kriegsschiffen gekämpft wird, sondern mit Spionage, Propaganda und anderen in der Regel nichttödlichen Methoden. Das trifft auf die digitalen Scharmützel der Gegenwart durchaus zu. Die weit überwiegende Zahl aller bekanntgewordenen Cyberangriffe und digitalen Schachzüge von Staaten sind eher dem Bereich Spionage und Propaganda zuzurechnen. Ein aktuelles Beispiel: die Publikation von E-Mails des Nationalkomitees der US-Demokraten mitten im Präsidentschaftswahlkampf, lanciert über die Enthüllungsplattform WikiLeaks. Nach Ansicht von IT-Sicherheitsunternehmen und US-Behörden war dies das Werk russischer Geheimdienste, mit der Absicht, die Chancen des republikanischen Kandidaten Donald Trump zu erhöhen. In die andere Richtung dürfen weite Teile dessen, was Edward Snowdens Dokumentenschatz über die tatsächlichen Aktivitäten der NSA und ihrer Verbündeten enthüllt hat, als digitale Spionage gelten, nicht als offensive, kriegerische Handlungen. Von einem kalten Cyberwar zu sprechen, führt aber womöglich dennoch eher in die Irre, und zwar aus zwei Gründen.

Zum einen betreffen die Auseinandersetzungen, in die mit digitalen Mitteln eingegriffen wird, nicht zwei Blöcke aus Supermächten und ihren Verbündeten: Die multipolare Welt von heute hat auch multiple Schlachtfelder für derartige Propaganda- und Spionageaktivitäten geschaffen. Man denke neben dem Antagonismus USA-Russland etwa an den zwischen Nord- und Südkorea, zwischen Nordkorea und den USA, zwischen China und den USA und so weiter. In all diesen Bereichen hat es Zwischenfälle gegeben, die die eine Seite der an-

deren zuschreibt, etwa das Abschöpfen großer Datenmengen, die Veröffentlichung geheimer oder privater Informationen oder Angriffe, die Rechnersysteme großer Banken und TV-Sender lahmlegten, so geschehen in Südkorea. Dass sich ein Angreifer zu Cyberaktivitäten bekennt, kommt aber so gut wie nie vor.

Geht man von einer historischen Analogie zum Kalten Krieg zwischen den NATO- und den Warschauer-Pakt-Staaten aus, fehlt den digitalen Scharmützeln vor allem ein wesentlicher Faktor: die Atomkriegsdimension beziehungsweise das Prinzip der „mutually assured destruction". Niemand weiß genau, was der Gegner jenseits von Propaganda und Spionage mit digitalen Mitteln anrichten kann. Dass aber irgendein Staat in der Lage ist, einen anderen mit den Mitteln des Cyberwar ähnlich zu verwüsten wie mit einem Atomschlag, erscheint aus heutiger Sicht höchst unwahrscheinlich.

Cyberangriffe werden immer einfacher

Richtig ist: Straftaten und Spionageangriffe, in denen das Internet eine Rolle spielt, nehmen dramatisch zu. Allein das Ausmaß der Datenlecks, die große Unternehmen von Sony bis Yahoo in den vergangenen Jahren eingestehen mussten, ist atemberaubend. Millionen von Nutzerdatensätzen werden auf entsprechenden Schwarzmarktplattformen zum Kauf angeboten, immer wieder müssen Firmen ihre Nutzer warnen und anhalten, Passwörter zu ändern und Sicherheitsüberprüfungen durchzuführen.

Mit Krieg hat all das aber wenig bis gar nichts zu tun. Der wohl größte bekanntgewordene Coup gegen eine staatliche Einrichtung, das amerikanische Office of Personnel Management (OPM), lieferte den Angreifern zwar umfang-

reiche Informationen über Millionen US-Beamte, auch über solche, die sich um eine Freigabe zur Einsicht in Geheiminformationen bemüht hatten, also etwa Mitarbeiter von Geheimdiensten. Ein kriegerischer Akt im Sinne der bewussten Zerstörung war aber auch dieser Angriff nicht.

Bekannt gewordene Cyberangriffe, bei denen tatsächlich Material oder gar Menschen zu Schaden gekommen sind, kann man weiterhin an einer Hand abzählen. Das prominenteste Beispiel ist bis heute Stuxnet, der ausgeklügelte Hightech-Virus, mit dem vermutlich eine Allianz aus US- und israelischen Geheimdiensten erfolgreich das iranische Atomprogramm sabotierte. Stuxnet ist ein gutes Beispiel, weil der Fall zeigt, welchen ungeheuren Aufwand die Angreifer betreiben mussten, um schließlich Zentrifugen zur Urananreicherung in der iranischen Anlage in Natans zu zerstören und ihr Wirken möglichst effektiv zu verschleiern. Stuxnet war in Wirklichkeit ein verschachteltes System diverser Schadprogramme, das auf unterschiedliche Hard- und Software einwirkte, dabei diverse, bis dahin unbekannte Sicherheitslücken ausnutzte, gestohlene digitale Signaturen von zwei Unternehmen einsetzte und schließlich ein Siemens-System zur Steuerung von Industrieanlagen befiel und manipulierte.

Die Sabotagewaffe muss Abermillionen gekostet, ihre Entwicklung ein ganzes Team von Fachleuten viele Monate beschäftigt haben. Dass Angriffe dieser Kategorie heute einfacher geworden sind, als sie 2010 waren, darf bezweifelt werden, denn Stuxnet dürfte für viele Unternehmen und Regierungen ein Weckruf gewesen sein, mit kritischer Infrastruktur noch weit sorgsamer umzugehen. Wie viel man bislang aus solchen Vorfällen gelernt und welche Sicherheitsmaßnahmen tatsächlich bereits umgesetzt wurden, ist allerdings eine offene Frage. Mehr Sensibilität für diesen Bereich ist zweifellos angezeigt.

Denn das „Internet der Dinge“, also die immer stärkere Vernetzung von Komponenten der Industrieproduktion ebenso wie von Alltagsgegenständen, bietet neue Einfallstore für digitale Angriffe. Bei der Konzeption und Einrichtung solcher Technologien, vom Smart Home über selbstfahrende Autos und Lkw bis hin zur vollvernetzten Fabrikanlage muss mehr Wert auf Sicherheit gelegt werden, als das derzeit vielfach der Fall ist. Sonst wächst tatsächlich die Gefahr von Cyberattacken, die realweltliche, gravierende Auswirkungen haben können.

Wir befinden uns bereits mitten im Cyberwar

Nur wenn man auch Propaganda und Spionage als kriegerische Handlungen betrachtet – siehe oben. Was wir gerade tatsächlich erleben, ist ein digitales Wettrüsten. Dieser Aufbau offensiver und defensiver Kapazitäten der digitalen Kriegführung unterscheidet sich in einem wesentlichen Punkt von anderen Formen der Aufrüstung: Es geschieht nahezu unsichtbar. Silos für Interkontinentalraketen lassen sich schwer verstecken, das Gleiche gilt für Panzerverbände oder Flotten. Die Offensivkapazitäten, die, nach allem, was wir aus NSA-Dokumenten wissen, von NSA und dem US Cyber Command bis-

lang aufgebaut worden sind, bleiben aber verborgen. Da werden Hintertüren in Hard- und Software eingebaut, Datenströme bei Bedarf mit Hilfe versteckter Router umgeleitet, Schadsoftware unbemerkt in normale Webseiten-Aufrufe eingeschleust. Es kann kein Zweifel bestehen, dass auch China, Russland, Nordkorea und viele andere Staaten mit unterschiedlichem Erfolg und unterschiedlichem Aufwand am Aufbau entsprechender Möglichkeiten arbeiten – aber all das passiert im Unsichtbaren. Gleichzeitig wächst die Nervosität auf allen Seiten. Die US-Armee und -Luftwaffe etwa bereiten ihre Soldaten mittlerweile aktiv auf Situationen vor, in denen tatsächliche Kriegshandlungen von Cyberattacken flankiert werden.

Für normale Nutzer hat das digitale Wettrüsten einen unliebsamen Nebeneffekt: All die Hintertüren und Schleichwege, die Geheimdienste in Hard- und Software einbauen, machen Systeme für alle Nutzer unsicherer. Denn wenn eine Hintertür existiert, dann kann sie auch von einem anderen Angreifer gefunden und genutzt werden als dem, der sie eingerichtet hat. Das Ganze geht derzeit also vor allem auf Kosten normaler Nutzer und Unternehmen, die sich eigentlich auf die Sicherheitsarchitektur von Internet und Geräten verlassen können sollten.

Ein Beispiel: Das ARD-Magazin „Fakt“ berichtete kürzlich über offenbar von der NSA bestellte Hintertüren in Überwachungskameras eines Unternehmens namens NetBotz. Diese Überwachungskameras, die in hochsensiblen Bereichen wie Rechenzentren eingesetzt wurden, verfügen nicht nur über die Möglichkeit, Videobilder aufzuzeichnen, sondern auch über Mikrophone und zum Teil Messgeräte für Raumtemperatur und Luftfeuchtigkeit. Als der Bundesnachrichtendienst von den Hintertüren erfuhr, verschwieg er dies einem Geheimdokument von 2005 zufolge sogar dem für Spionageabwehr zuständigen Verfassungsschutz (BfV), aus Sorge vor politischen Auswirkungen einer solchen Offenlegung.

Auch hier gilt: Es geht um Spionage, nicht um Kriegshandlungen. Aber die Sicherheit auch deutscher Unternehmen und Organisationen, die entsprechende Technologie einsetzen, wird nicht nur durch die NSA, sondern womöglich auch durch Trittbrettfahrer kompromittiert.

Was wir brauchen, ist eine Art Kontrollabkommen über Cyberwaffen

Dem digitalen Wettrüsten mit digitalen Abrüstungsverhandlungen zu begegnen, wäre in der Tat wünschenswert. Derzeit scheint sich der Umgang mit dem Thema auf die Frage zu beschränken, ob ein Cyberangriff denn nun juristisch mit einem kinetischen, also einem mit Bomben, Raketen oder Schusswaffen durchgeführten gleichzusetzen sei oder nicht. Dabei sollte es nicht bleiben – höchste Zeit, dass die digitalen Supermächte der Gegenwart wenigstens damit beginnen, gemeinsame Rahmenbedingungen für den Einsatz von digitalen Waffen zu erarbeiten. Denn natürlich könnte etwa das Lahmlegen eines

nationalen Strom- oder Transportnetzes, sofern überhaupt möglich, massive Folgen haben, Volkswirtschaften schädigen und auch Menschenleben kosten.

Ein Problem dabei ist eines, das dem ganzen Bereich ohnehin innewohnt: die Schwierigkeit der Attribution. Wo eine Interkontinentalrakete abgeschossen wurde, lässt sich kaum verschleiern; bei Cyberattacken dagegen können die Angreifer ihre Spuren unter Umständen so gründlich verwischen oder sogar falsche Fährten legen, dass die Urheber allenfalls vermutet werden können. Über geheimgehaltene Fähigkeiten und Aktionen Abrüstungsverhandlungen zu führen, dürfte sich aber als schwierig erweisen.

Zum Fall Stuxnet etwa hat sich bis heute niemand offiziell bekannt, obwohl es kaum noch Zweifel an der Urheberschaft gibt. Bei Cyberangriffen und Spionageattacken sind Verschleierung und falsche Fährten nicht die Ausnahme, sondern die Regel, egal, wer der tatsächliche Urheber ist. All das hat nicht zuletzt damit zu tun, dass die beschriebenen Aktivitäten bislang überwiegend die Domäne von Geheimdiensten zu sein scheinen. Militärische Cyberangriffe, die etwa die digitalen Systeme feindlicher Streitkräfte in einem bewaffneten Konflikt lahmlegen sollen, sind bislang noch nicht klar belegt worden.

Gerade Deutschland ist für einen Cyberwar nicht im Geringsten gerüstet

Das ist derzeit vermutlich wahrer, als es den Verantwortlichen im Verteidigungs-, aber auch im Innenministerium lieb sein kann. Die digitalen Fähig- und Fertigkeiten deutscher Beamter und Soldaten sind offenbar nicht so ausgeprägt, wie man es sich von einer Hightech-Nation wie Deutschland erwarten würde. Man kann dem Verteidigungsministerium aber zugutehalten, dass dieses Defizit mittlerweile erkannt wurde: Im April 2016 stellte Verteidigungsministerin Ursula von der Leyen ihre Pläne für einen neuen Organisationsbereich für den „Cyber- und Informationsraum" vor. Auch im Ministerium selbst wurde bereits eine neue Abteilung namens Cyber/IT eingerichtet.

Insgesamt wird der Bereich bei der Bundeswehr mit 13 500 Stellen ausgestattet. Für Cyberoperationen und Cybersicherheit werden zwei neue Bundeswehrzentren eingerichtet. Am 1. April 2017 soll ein Generalleutnant als Inspekteur die Führung des Kommandos übernehmen. Das Ministerium betonte bei der Vorstellung des neuen Bereichs, dass für Einsätze „auch im Cyber- und Informationsraum selbstverständlich der Parlamentsvorbehalt" gelte.

Wie erfolgreich die Anwerbekampagne der Bundeswehr für IT-Fachkräfte mit dem Slogan „Mach, was wirklich zählt" war, ist bislang aber unklar. Die Bundeswehr konkurriert auf diesem Gebiet mit zahlungskräftigen Unternehmen um rare und gefragte Bewerber.

Dass derzeit, was die IT-Sicherheit bundesdeutscher Institutionen angeht, einiges im Argen liegt, zeigte 2015 der sehr erfolgreiche Angriff auf das Netz des Deutschen Bundestags: Über Wochen hinweg, wenn nicht über Monate, konnten die Angreifer – nach Einschätzung des Bundesamts für Verfassungs-

schutz aus Russland – Daten aus den Rechnern von Bundestagsabgeordneten und ihren Mitarbeitern sowie aus Parlamentsservern ausleiten. Nachdem der Angriff entdeckt worden war, dauerte es Monate, ihn zu bekämpfen und die Systeme entsprechend abzusichern. Noch heute benutzen die meisten Abgeordneten nicht einmal die in ihren E-Mail-Programmen eingebaute Verschlüsselungstechnik, auch nicht für die Kommunikation untereinander.

Mit anderen Worten: Auch jenseits echter Kriegsszenarien ist in Sachen Cybersicherheit in Deutschland noch viel Aufbauarbeit zu leisten, und zwar auf allen Ebenen. Um den anhaltenden Mangel an Fachkräften zu beheben, wird man wohl früher ansetzen müssen, nämlich bereits bei der Hochschulausbildung.

Ein gigantischer Cyberangriff ist nur noch eine Frage der Zeit

Diese These wird sich hoffentlich als falsch erweisen. Dagegen sprechen die bisherigen Erfahrungen in diesem Bereich – Stuxnet hat Zentrifugen in einer einzigen Anlage zerstört, kein nationales Stromnetz lahmgelegt. Ob sich ein solches Szenario, wie es bislang nur in Krimis und Hollywoodfilmen vorkommt, tatsächlich real umsetzen ließe, ist derzeit völlig unklar.

Gleichzeitig dürfte zumindest Regierungen rund um die Welt klar sein, dass ein wirklich verheerender Cyberangriff, sollte er sich doch durchführen lassen, von den Betroffenen als Kriegserklärung aufgefasst werden dürfte. Die USA, aber auch die deutsche Bundesregierung etwa haben sich in dieser Hinsicht schon sehr klar positioniert: Ein schwerer Cyberangriff kann demnach ebenso als kriegerischer Akt gewertet werden wie etwa ein Luft- oder Raketenangriff. Einen solchen Angriff würden wir demnach wohl erst dann sehen, wenn die Zeichen auch sonst auf Krieg stünden – was Politik und Diplomatie hoffentlich zu verhindern wissen werden.

Anders sieht es im Hinblick auf terroristische Organisationen aus: Bei ihnen wäre die Hemmschwelle, mit einer Cyberattacke große Schäden anzurichten, zweifellos niedrig. Doch dass etwa der so genannte Islamische Staat in der Lage wäre, tatsächlich Cyberoperationen von der Qualität des Stuxnet-Virus durchzuführen, ist derzeit nicht zu erkennen und auch eher unwahrscheinlich.

Nach derzeitigem Stand ist ein gigantischer Cyberangriff also glücklicherweise nicht wahrscheinlicher als ein neuer Weltkrieg.

Prof. Christian Stöcker baut an der HAW Hamburg den neuen Masterstudiengang „Digitale Kommunikation“ auf. Zuvor war er Netzwelt-Ressortleiter bei Spiegel Online.