Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260

Herausgegeben von Stefan Schumacher und Jan W. Meine

Meine Verlag Magdeburg

Dieser Artikel erscheint in der Serie „Informationstechnik und Sicherheitspolitik. Wird der dritte Weltkrieg im Internet ausgetragen?“ Herausgegeben von Jörg Sambleben und Stefan Schumacher.

Sicherheitsumfeld Cyber-Space: Abhängigkeiten, Akteure, Herausforderungen und Perspektiven

Felix F. Seidler

In diesem Artikel wird der Wandel der Sicherheitspolitik im Cyber-Space, ausgehend von einer zunehmenden Vernetzung sämtlicher elektronischer Geräte, thematisiert. Die staatliche Sicherheitspolitik bleibt davon zukünftig nicht unberührt.

Zitationsvorschlag: Seidler, Felix F. (2011). Sicherheitsumfeld Cyber-Space: Abhängigkeiten, Akteure, Herausforderungen und Perspektiven. Magdeburger Journal zur Sicherheitsforschung, Band 2, 2011, S. 102–114.

http://www.wissens-werk.de/index.php/mjs/article/viewFile/107/77

Einleitung

Die Teilnahme des Facebook-Gründers Mark Zuckerberg am G8-Gipfel 2011 dürfte letzte Zweifel am Stellenwert von Cyber-Sicherheit ausgeräumt haben. Dass ein junger Firmengründer den Mächtigen der Welt beim Verständnis ihres neuen (sicherheits-)politischen Umfelds half, kennzeichnet den Wandel der Sicherheitspolitik im Cyber-Space zu Lasten der etablierten Politik. Enorme Verschiebungen zu Lasten staatlicher Sicherheitspolitik sind, ausgelöst durch das Netz, in vollem Gange. Welchen Stellenwert wird Cyber-Sicherheit zukünftig erhalten? Was bedeutet Sicherheit im Netz? Welche Akteure dominieren die elektronische Zukunft? Kann die Politik mit der Technik Schritt halten? Die Antworten auf diese und vor allem die letzte Frage werden für Politik und Gesellschaften in der Zukunft entscheidend sein.

Der Begriff Cyber bedeutet vernetzte elektronische Informationssysteme. Die Gesamtheit aller vernetzten, elektronischen Informationssysteme, „sämtliche Computernetze der Welt und alles, was sie steuern und miteinander verbinden“,[1] bilden wiederum den Cyber-Space inklusive des Internet.

Die Begriffe Cyber-Space und Internet werden oft wechselseitig und damit irreführend verwendet. An oberster Stelle steht jedoch der Begriff des Cyber-Space, denn das Internet ist Teil dessen, nicht aber umgekehrt. Beispielsweise sind die internen Computersysteme des Pentagon nicht Teil des offenen World Wide Web, aber natürlich Teil der Gesamtheit vernetzter elektronischer Informationssysteme, also des Cyber-Space. Dabei ist der Cyber-Space sowohl physischer (Bsp.: PCs, Glaserfaserkabel, USB-Sticks, Hardware) wie nicht-physischer Natur (Bsp.: WLAN, UMTS, Satellitenübertragung, Software). Das heißt auch, Attacken und Sicherheit im Cyber-Space sind nicht kinetischer Natur, können aber kinetische Folgen nach sich ziehen.

Ein derartiges Umfeld lässt keine absolute Sicherheit zu. Sicherheit, „die Gewissheit der eigenen Unversehrtheit“,[2] kann es im Cyber-Space deswegen nicht geben, weil Gewissheit nicht herstellbar ist. Bis heute gilt nach Hauptmann Christian Czosseck vom NATO-CCDCOE[3] die Regel: „Jede Software hat Schwachstellen“.[4] Da Politik, Militär, Wirtschaft, Organisationen, private Haushalte und unzählige andere Akteure täglich Software benutzen und von dieser abhängig sind, können sich diese niemals gewiss sein, dass ihre elektronischen Systeme unversehrt bleiben. Durch den anhaltenden technischen Fortschritt ist ein Ende dieser Entwicklung nicht absehbar, so dass die Verwundbarkeit ganzer Gesellschaften stetig wächst, denn „mit größerer Abhängigkeit geht größere Verwundbarkeit einher“.[5]

Sicherheitsumfeld Cyber-Space

Asymmetrie, die Ungleichmäßigkeit von Akteuren, Gegenständen und Prozessen, ist elementarer Bestandteil des Sicherheitsumfelds Cyber-Space. Die Asymmetrie beginnt zwischen Mensch und Maschine

1 Clarke, R. & Knake, R. (2011). World Wide War. Angriff aus dem Internet, S. 103.

2 Zangl, B. & Zürn, M. (2003). Frieden und Krieg, S. 172.

3 Cooperative Cyber Defence Centre of Excellence.

4 Zitiert nach: Schuller, K. (2010). „Das fünfte Schlachtfeld“: Der Spion, der aus dem Cyberspace kam. In: http://www.faz.net/s/RubFC06D389EE76479E9E76425072B196C3/Doc~E2CFCE11426824B73A0981CE25C58CAD7~ATpl~Ecommon~Scontent.html (20.06.2011).

5 Yorke, C. (2010). Cybersecurity and Society: bigsociety.com. The World Today, 66 (12), 19. Alle Übersetzungen aus dem Englischen durch den Autor.

und setzt sich in der Interdependenz unterschiedlichster, sowohl von Menschen bedienter wie automatisierter IT-Systeme fort. Ungleich sind ebenfalls der rapide Ereignisdruck und die dazu verhältnismäßige Langsamkeit politischen Handelns. Das allein durch die Geschwindigkeit der Datenübertragung sehr schnelllebige Sicherheitsumfeld Cyber-Space trifft auf sicherheitspolitische Strukturen, etwa in Regierungen, Parlamenten und Bürokratien, die aus ihrer Natur heraus, zum Beispiel in langen Gesetzgebungs- oder Verwaltungsverfahren, nicht zur schnellen, unmittelbaren Reaktion in der Lage sind. Im Prozess zur Herbeiführung einer Reaktion ist die Politik jedoch von vernetzten elektronischen Systemen abhängig. Die Datenströme der Politik sind wie alle anderen Datenströme des Cyber-Space überwach-, manipulier- und unkontrollierbar. Deswegen laufen konventionelle Schutzstrategien wie Prävention und Abschreckung ins Leere, zumal jedes Handeln von Akteuren im Cyber-Space einer immensen Asymmetrie in Fehlertoleranz und Wirkung ausgesetzt ist.

Akteure können im Cyber-Space als aktive oder passive Figuren in Erscheinung treten. Zu differenzieren sind an dieser Stelle „Cyber-Spionage" und „Cyber-War". Ersteres bezieht sich auf ein passives Abfangen oder Überwachen von Informationen und Daten, wie etwa das Mitlesen von E-Mails oder das Ausspähen elektronischer Finanztransaktionen. Cyber-War bedeutet stattdessen, dass eine aktive Handlung vorgenommen wird. In diesem Fall würden die E-Mail oder Finanztransaktion nicht überwacht, sondern bewusst sabotiert. Neben der Software kann sich Cyber-Spionage/-War auch die Hardware betreffen. Beispiele sind das Abzapfen von Daten mittels Abhöreinrichtungen oder ein Cyber-Angriff zur Zerstörung eines Serverzentrums oder Unbrauchbarmachung eines Kampfjets.

Nicht übersehen werden darf die Kluft zwischen den Akteuren Mensch und Maschine. Die moderne Technologie ermöglicht es, macht es sogar wahrscheinlich, dass der Anwender die Maschine, die er bedient, über die bloße Bedienung hinaus nicht versteht. Es kommt daher häufig vor, dass ein Mensch annimmt, er bediene ein elektronisches Gerät oder eine Software richtig; fühlt sich daher seiner eigenen Unversehrtheit gewiss**.** Tatsächlich bedient dieser Mensch Gerät oder Software durch unbewusstes Fehlverhalten oder Unwissen fehlerhaft, genießt also entgegen seiner Wahrnehmung keine Sicherheit, sondern vergrößert durch die Fehlbedienung womöglich noch die Sicherheitslücken. Dies schließt nicht nur Bedienung, sondern auch die Installation der Technik mit ein. Der Mensch kann also durch Unverständnis und unbewusstes Fehlverhalten für sich selbst zum Sicherheitsrisiko werden. Die Technologie ist demgegenüber „agnostisch zu Politik und Ideologie"[6] und menschlichem Verhalten generell. Automatisierte Systeme und Warnsysteme können diese Kluft teilweise überbrücken, indem sie den Menschen auf Installations- oder Anwendungsfehler hinweisen, aber auch diese Kontrollsysteme sind auf die richtige Handhabung durch Menschen angewiesen.

Es existiert also eine Kluft, indem einerseits die Maschine bzw. deren Software das Handeln des weniger wissenden Menschen anleitet oder andererseits hoch spezialisierte Menschen in der Lage sind, Hard- und Software zu kontrollieren. Ein Beispiel bietet der elektronische Börsenhandel.

6 Lord, K. & Sharp, T. (2011). America's Cyber Future: Security and Prosperity in the Information Age Vol. I, S. 20. In: http://cnas.org/files/documents/publications/CNAS_Cyber_Volume%20I_0.pdf (23.06.2011).

Broker können Transaktionen über Laptop mit WLAN oder Smartphone abwickeln ohne sich der Verwundbarkeit von Geräten wie Datenübertragungsweg bewusst zu sein. Im Gegensatz dazu haben Spezialisten „Algorithmen ersonnen, die diese großen Tranchen in viele kleine Transaktionen aufteilen, die mit Millisekunden Unterschied Aktienpakete am globalen Aktienmarkt platzieren“,[7] also auf die Aktionen der Händler reagieren und so genau die Kluft des Wissens zwischen Maschinen und Anwendern ausnutzen. Andere Spezialisten entwerfen natürlich Programme, die solche Aktionen registrieren. So vergrößert sich einerseits im Börsenhandel die Kluft zwischen Mensch und Maschine auf das Handelsgeschehen sowie die Kluft zwischen wissenden und unwissenden Marktteilnehmern.

De facto stellt das Sicherheitsumfeld Cyber-Space eine infinit-polare Weltordnung dar. Während die Anzahl der Staaten, sprich Pole, in politikwissenschaftlichen Debatten um die uni-, bi- und multipolare Weltordnung aktuell nach der Unabhängigkeit des Südsudans auf 193 begrenzt ist, kann man im Cyber-Space keine quantitative Grenze der möglichen Pole ausmachen. Stattdessen verändert sich die Zahl der Pole bestehend aus privaten, kommerziellen und staatlichen Akteuren quasi täglich. Außerdem definierten sich die bisherige Weltordnung und das Sicherheitsumfeld von Gesellschaften zu hohem Maße über Geografie. Während ein Staat wie Luxemburg durch seine geografische Lage keine Sicherheitsrisiken zu befürchten hat, gilt dies für Katar am Persischen Golf nicht. Im Cyber-Space ist dieser Unterschied in der Theorie aufgehoben und beide den gleichen Risiken ausgesetzt. Den Unterschied macht in der Praxis die Eintrittswahrscheinlichkeit aus, also inwieweit dieser Staat ein potenzielles Ziel für andere darstellt. Diese Wahrscheinlichkeit definiert sich wieder über Geographie, dann Katar wäre aufgrund seiner geographischen Lage, mit einem Blick gen Iran, eher ein Ziel für Cyber-Angriffe als Luxemburg.

Komplexität und Interdependenz der Cyber-Systeme

Bis hierhin lässt sich feststellen, der Cyber-Space ist ein Raum massiver gegenseitiger Abhängigkeiten. Für Laien wie viele Fachleute, wie später dargestellt wird, sind diese Interdependenzen weitestgehend undurchschaubar. Das beginnt bei den Netzen, denn Regierungen wie Firmen mögen zwar eigene Netze unterhalten, sind aber für ihr gesamtes Handeln im Cyber-Space auf private, kommerzielle Anbieter, denen Technik und Netz inklusive Kontrollmöglichkeiten gehören, angewiesen.

Regierungen und Parlamente verfügen zwar über die Möglichkeit gesetzlicher Regulierung, aber angesichts des Tempos der Entwicklungen im Netz, etwa bei Fragen des Datenschutzes bei Facebook und Google, zeigen sich die engen Grenzen politischen Handelns. Stattdessen können Staatsapparate das „Tempo des Netzes nicht mithalten“.[8] Gleiches gilt für gewöhnliche private Nutzer, wenngleich diese prinzipiell schneller als staatliche Bürokratien in der Lage sind, sich an neue Entwicklungen anzupassen. Große Unternehmen ändern ihren Umgang mit Kundendaten, wobei die Kunden sich dessen häufig gar nicht bewusst sind, nach Belieben. Die Entwicklungen laufen auch hier so schnell ab, dass es dem gewöhnlichen Nutzer schwer

7 Wittkewitz, J. (2011). Cyberwar: Alles wird zur Ware. http://www.faz.net/artikel/C30833/cyberwar-alles-wird-zur-ware-30443353.html (23.06.2011).

8 Lord, K. & Sharp, T. (2011). America's Cyber Future, S. 32.

fallen dürfte, alle Entwicklungen unmittelbar nachzuvollziehen.

Ereignisdruck ist also ein bestimmender Faktor des Umfeldes Cyber-Space weit über die Sicherheitspolitik hinaus. Den handelnden Akteuren bieten sich dabei nur sehr kurze Reaktionszeiten, um mit den Entwicklungen von Cyber-Angriffen oder dem Datenschutz mitzuhalten. Die „Zerstreuung der Macht im Cyber-Space“[9]verschiebt unter dem Eindruck der kurzen Reaktionszeiten die Machtverteilung deutlich zu Ungunsten des Staates. Durch geringe Reaktionszeiten steigt natürlich die Verwundbarkeit der Akteure durch Cyber-Attacken und das Risiko, heimlicher Überwachung oder Manipulation zum Opfer zu fallen.

In dem System des Cyber-Space „verschwimmen die Trennlinien“[10]der bisherigen Dimensionen staatlichen Handelns. Da ein Computervirus, wie Stuxnet, nicht zwischen zivil oder militärisch genutzten Rechnern unterscheidet, gibt es keine Trennlinie zwischen ziviler und militärischer Defensive aber auch Offensive.[11] Die Aufhebung aller geografischen Grenzen verschärft diese Situation zusätzlich, da sowohl Ziele wie Angreifer extrem schnell auftauchen und verschwinden können. In der Offensive könnten sowohl zivile, geheimdienstliche wie militärische Stellen versuchen, Seiten mit extremistischem Inhalt zu löschen. Nichtsdestotrotz kann der Seitenbetreiber, wenn er den Vorgang bemerkt, die Dateien selbst aus dem Netz nehmen, damit verschwinden, aber später das Material erneut ins Netz stellen. Selbst wenn die Löschung gelingt, kann das Datenmaterial wieder auftauchen, solange der Betreiber der Website Kopien auf anderen Datenträgern besitzt. Kontroll- und Überwachungsaufgaben ziviler und militärischer Stellen korrelieren daher unabhängig von ihren gesetzlichen Rahmenbedingungen alleine durch die Natur des Cyber-Space miteinander. Die Folge ist, dass die Politik kein Problem im Cyber-Space alleine lösen kann.

Auswirkungen auf das staatliche Schutzversprechen

Aufgabe demokratischer Staatswesen ist es, mittels Ausübung von Staatsgewalt dem Souverän dessen Sicherheit auf dem eigenen Staatsgebiet zu garantieren. Da der Staat allerdings zur Erfüllung dieser Aufgabe von Systemen abhängig ist, die ohne räumliche Begrenzung einer unquantifizierbaren Zahl von Akteuren Angriffsfläche bieten, stellt sich die Frage, inwieweit dieses Versprechen noch haltbar ist. Außerdem bewegt sich der Souverän im Cyber-Space ohne jeden Bezug zum Hoheitsgebiet, was das territorialbezogene, staatliche Schutzversprechen im Cyber-Space ad absurdum führt. Nur Schutzreaktionen auf die physischen Folgen von Cyber-Attacken kann der Staat weiterhin versprechen.

Staatliche Sicherheitsorgane in Demokratien bedienen sich zur Einhaltung des Schutzversprechens der Mittel Abschreckung und Abwehr. Abschreckung meint das Einwirken des Staates auf den Willen eines potenziellen Aggressors bestimmte Handlungen einzustellen oder zu unterlassen, indem man dem Aggressor deutlich macht, dass dieser dabei durch sein Handeln „mehr zu verlieren als zu gewinnen, zumindest aber nicht die von ihm erwartenden Vorteile erlangen würde“.[12] Abschreckung kann nur

9 Nye, J. (2011). Power and National Security in Cyber-Space, S. 9. http://www.cnas.org/files/documents/ publications/ CNAS_Cyber_Volume%20II.pdf (24.06.2011).

10 Lord, K. & Sharp, T. (2011). America’s Cyber Future, S. 23.

11 Lord, K. & Sharp, T. (2011). America’s Cyber Future, S. 32.

12 Meier, E., Roßmanith R. & Schäfer, H. (2003).

dann erfolgreich sein, wenn der Staat den potenziellen Aggressor von seiner Fähigkeit und seinem Willen überzeugt, „Mittel der Vergeltung anzuwenden, wenn der andere eine bestimmte Linie überschreitet".[13]

Alleine durch die geografische Entgrenzung des Cyber-Space laufen diese herkömmlichen, auf physischen Mitteln des Staates basierenden Strategien ins Leere. Um konkret auf einen potenziellen Aggressor einwirken zu können, muss die Existenz dieses Aggressors bekannt sein. Im Falle einer Gegnerkonstellation Staat-Staat oder Staat-Terrororganisation besteht theoretisch ein physisches Gegenüber. Während Staaten Truppenverlegungen oder Waffenkäufe mit technischen Mitteln verhältnismäßig leicht nachvollziehen können, kann sich ein Aggressor, auch dies können aber wieder Staaten oder Terrororganisationen sein, im Cyber-Space unbemerkt auf eine Aggressive Handlung vorbereiten, deren Natur dem Staat noch nicht einmal bekannt sein muss. Es fehlt also auf der Seite des Staates das Wissen um die Existenz potenzieller Aggressoren, womit konkrete Abschreckungsmaßnahmen über allgemeine Abschreckungsstrategien hinaus unmöglich werden. Außerdem können Willen und Handlung eines Aggressors im Cyber-Space, wie etwa bei einem Angriff eines einzelnen Hackers auf ein staatliches Computernetzwerk, vom zeitlich so extrem kurzer Dauer sein, dass sich dem Staat gar nicht die Möglichkeit bietet in irgendeiner Form darauf einzuwirken. Die Schlussfolgerung ist also, die Politik wird je weniger in der Lage sein das staatliche Schutzversprechen einzuhalten, je weiter der technische Fortschritt geht. Auch Mittel der Vergeltung eines Staates leiden darunter, dass der Staat bei Schaffung dieser Mittel den Aggressor nicht kennt. Letzterer jedoch leichter erfahren, was für Mittel der Vergeltung einem Staat zur Verfügung stehen und sich darauf vorbereiten.

Die Logik „mehr zu verlieren als zu gewinnen" greift für die Anwendung durch die Politik zur Abschreckung ebenfalls nicht. Materieller Verlust, also unbrauchbare Hardware, ist leicht und billig ersetzbar. Ein wie auch immer gearteter politischer, juristischer, finanzieller oder sozialer Verlust der anderen Seite bedingt nur deren zweifelsfreie Identifizierung in sehr kurzer Reaktionszeit, sondern auch Fähigkeit und Willen diesen Verlust außerhalb das Cyber-Space, also wieder innerhalb geografischer und territorialer Grenzen herbeiführen zu können. Dem Berliner IT-Sicherheitsforscher Sandro Gaycken greift „eine aktive präventive Abschreckung durch Strafverfolgung oder Vergeltung" im Sicherheitsumfeld Cyber-Space nicht.[14]

Im gleichen Satz betont Gaycken, dass selbiges auch für „eine passive direkte Abwehr nach dem Prinzip des Schutzwalls" gilt. In interdependenten und komplexen Netzen bedarf es allerdings nicht eines Schutzwalls, sondern vieler Schutzwälle. Jedem dieser elektronischen Schutzwälle müssten alle Arten von Cyber-Attacken bekannt sein. Deren Charakter verändert sich aber allein schon durch die laufende Fortentwicklung von Software ständig. Kenneth Geers vom NATO-CCDCOE nach werden täglich „etwa 15 Schwachstellen bei Computer-Programmen gefunden, etwa 40 Internetseiten in Deutschland mit Viren infiziert [und] alle zwei Sekunden entsteht ein neu-

Wörterbuch zur Sicherheitspolitik, S. 12.

13 Dunn Cavelty, M. (2011). Cyber-Allies. Strengths and weaknesses of NATO´s cyberdefense posture. Internationale Politik Global Edition, 2011 (3), S. 13.

14 Gaycken, S. (2011). Krieg der Rechner. Warum es so schwierig ist, sich vor militärischen Cyber-Angriffen zu schützen. Internationale Politik, 2011 (2), S. 88.

es Computer-Virus".[15] Neben der dauerpräsenten Möglichkeit des Softwareeinbruchs, besteht auch die Möglichkeit des Hardwareeinbruchs, der „wesentlich schwerer zu entdecken und schwieriger abzuwehren als ein Softwareeinbruch".[16] Allerdings steht die Möglichkeit des Hardwareeinbruchs aufgrund der Notwendigkeit von Zugang und Ressourcen am ehesten Staaten mit ihren Nachrichtendiensten oder „Insidern" zur Verfügung.

Die Bemühungen des Staates sein Schutzversprechen im Cyber-Space einzuhalten, sind also darauf reduziert, da der Staat Gewissheit nicht herstellen kann, zumindest den Anteil an Ungewissheit über die eigene Unversehrtheit nicht zu groß werden zu lassen. Zusammengefasst bedeutet dies, die Politik kann nur erreichen, dass das Umfeld für ihren Souverän *sicherer*, nicht aber *sicher* wird.

Diffuses Feld an Akteuren, Manipulierbarkeit und Asymmetrie

Jeder, der an den Cyber-Space angeschlossen ist, gleich ob Staat, Unternehmen, Gruppe oder Individuum, kann theoretisch Urheber wie Ziel von Cyber-Angriffen sein. Was dieses Feld an Akteuren so diffus macht, ist, dass gerade der Angreifer oft nicht identifizierbar ist, nur selektiv oder einmalig in Aktion tritt oder im Falle von Gruppen oder Netzwerken seine Zusammensetzung laufend ändert.

Wenn ein einzelner Hacker sich nach einem oder mehreren Angriffen von seinem Tun verabschieden und danach nie wieder in Erscheinung treten kann, bleibt er so dem Zugriff anderer Akteure, vor allem staatlicher Organe entzogen. In politischen oder terroristischen Gruppen kann die Zusammensetzung der beteiligten Personen schnell wechseln, wobei sich die Beteiligten hier noch persönlich kennen, so dass mit konventioneller nachrichtendienstlicher oder polizeilicher Arbeit Aufklärung denkbar bleibt. Anders ist dies in virtuellen internationalen Hackernetzwerken, wo sich die beteiligten oft nie persönlich begegnen und jeder Teilnehmer nach eigenem Ermessen über „ob" und „wie" seiner Teilnahme entscheiden kann, ohne dass es eine zentrale Steuerung gibt. Außerdem können all diese Teilnehmer frei darüber entscheiden wie viel sie von ihrer Identität preisgeben oder ihre Identität durch Manipulation verschleiern, womit es der Politik am Gegenüber fehlt, auf das aktiv, konkret eingewirkt werden könnte. Generelle und passive Maßnahmen wie Gesetze erzielen gegenüber solchen Akteuren mangels deren Fassbarkeit nämlich kaum eine Wirkung.

Einen Angreifer im Cyber-Space zu identifizieren ist außerordentlich schwierig. Bedingung ist, dass der Angegriffene die Attacke bemerkt sowie seine Schwachstelle und die Angriffssoftware identifiziert. Sofern der Angreifer dann Informationen hinterlassen hat, sind diese „nicht dauerhaft physisch",[17] was die Zurückverfolgung von Angriffen enorm erschwert. Gelingt es, den geografischen Ursprungspunkt oder den Ursprungsrechner eines Angriffs zu lokalisieren, sagt dies noch nichts über den eigentlichen Angreifer aus. Dass ein Computer in einem bestimmen Land steht, beweist noch nicht, dass dessen Regierung Urheber der Cyber-Attacke war. Außer-

15 Zitiert nach: Jiménez, Camilo (2010). Kriegsführung im Cyberspace: Unsichtbare Angriffe mit realen Folgen. http://www.sueddeutsche.de/digital/kriegsfuehrung-im-cyberspace-unsichtbare-angriffe-mit-realen-folgen-1.1003586-2 (25.06.2011).

16 Clark, W. & Levin P. (2009). Securing the Information Highway. How to Enhance the United States´ Electronic Defenses. Foreign Affairs, 2009 (6), S. 8.

17 Gaycken, S. (2011). Krieg der Rechner, S. 92.

dem sind die Akteure im Cyber-Space in der Lage fremde Rechner, ohne Wissen deren Eigentümer, für Angriffe zu kapern. Selbst wenn der schwierige Sprung über die Maschine-Mensch Schwelle bei der Identifizierung gelingt, sagt die Identifizierung des oder der Menschen hinter der Attacke noch nichts über deren eigentlichen Urheber aus. Ein Staat oder Unternehmen kann eine Gruppe oder einen einzelnen Hacker, ohne, dass diese wissen für wen sie eigentlich arbeiten, anheuern, um gegen andere Staaten oder Unternehmen Cyber-Angriffe durchzuführen. Gelänge es trotz des Ereignisdrucks und der kurzen Reaktionszeit einige der Angreifer sicher zu identifizieren, „wäre die Beweisführung, dass ein Staat (oder eine Terrororganisation) die Angriffe in Auftrag gegeben hat, das nächste Hindernis".[18] Dies zeigt sich gut an den Cyber-Attacken auf 103 Länder und internationale Organisationen aus dem Jahr 2009 oder dem Angriff auf Estland 2007, deren geografischer Ausgangspunkte zwar in China und Russland lokalisiert, aber staatliche Urheberschaft (offiziell) nicht bewiesen werden konnte.[19] Für die betreffenden Staaten blieben unmittelbare Konsequenzen daher aus. Ein Versuch der Beweisführung ist, über die Art des angegriffenen Ziels oder die gestohlenen Daten auf den Angreifer zu schließen. Militärische Daten oder Systeme entsprächen wohl am ehesten den Systemen von Staaten, während etwa die Systeme von Banken eher Kriminellen zuzuordnen wären. Allerdings kann sich jede Seite auch hinter solchen Interpretationen tarnen. Will ein Staat etwa zur Wirtschaftsspionage an die Daten einer Bank kommen, wird er natürlich die Wahrnehmung begrüßen, der Angreifer müsse unter den Kriminellen zu suchen sein. Nur bei extrem komplizierten Angriffen, wie Stuxnet, kann man sicher sein, dass ein Staat oder Staaten, in diesem Fall die USA und Israel,[20] aufgrund der notwendigen großen Ressourcen, der Urheber seien muss.

Für Staaten ist dies insoweit problematisch, als dass Rechtfertigungsdruck gegenüber anderen Staaten entsteht, warum der betreffende Staat nichts gegen die von seinem Territorium ausgehenden Cyber-Attacken tut. Letzterer hat wiederum ein Reputationsproblem, wenn er nicht in der Lage ist, sein Gewaltmonopol auszuüben und die Angriffe von seinem Territorium aus zu unterbinden. Auf der anderen Seite entstehen hier für Staaten als Aggressoren auch Vorteile, denn diese können glaubwürdige Abstreitbarkeit vortäuschen und sich dahinter verstecken, die Angriffe gingen von Kriminellen auf ihrem Territorium aus, gegen die man leider keine Handhabe habe. Ein Beispiel dafür bietet Russlands Antwort auf den Vorwurf, die Cyber-Angriffe 2007 auf Estland seien vom russischen Staat gekommen. Moskau behauptete stattdessen, russische „Patriotäten" hätten ohne Billigung der Regierung gehandelt.[21]

Durch die Asymmetrie von schwieriger Entdeckbarkeit bei gleichzeitiger billiger Effektivität sind Cyber-Attacken vor allem für Akteure mit offensiven Intentionen attraktiv. Dazu kommt die „Asymmetrie in der Fehlertoleranz: Angreifer dürfen tausende Fehler machen, Verteidiger keinen einzigen".[22] Auf andere Art und Weise wurde die Asymmetrie in der Fehlertole-

18 Dunn Cavelty, M. (2011). Cyber-Allies, S. 13.

19 Horowitz, M. (2010). A Common Future? NATO and the Protection of the Commons, S. 4. http://www.thechicagocouncil.org/userfiles/file/task%20force%20reports/Trans-Atlantic_Papers_3-Horowitz.pdf (25.06.2011).

20 Vgl.: Clarke, R. & Knake, R. (2011). World Wide War, S. 50ff.

21 Ebd., S. 34.

22 Gaycken, S. (2011). Krieg der Rechner, S. 90.

ranz während der arabischen Revolutionen deutlich. Die Oppositionellen in Tunesien, Ägypten, Libyen und Syrien brauchten nur einen einzigen freien elektronischen Kommunikationsweg aus ihren Land, während die Regime darauf angewiesen waren, jeden Weg zu blockieren. Die Auswirkungen der wenigen Lücken trugen zum Sturz der Regime bei.

Doch das wichtigste Prinzip „der neuartigen Cyberattacken ist ihre hohe Wirkasymmetrie: Mit einer geringen Ursache lässt sich eine immense Wirkung erzielen".[23] Dieses Prinzip wirkt sich zu Lasten der Staaten und zu Gunsten nicht-staatlicher Akteure aus. In den USA hat man bereits festgestellt, dass die "Amerikaner bisher Milliarden von Dollar für ihre [Cyber-]Verteidigung ausgeben habe, aber selbst diese großen Ausgaben ungenügend waren".[24] So steigt die Verwundbarkeit von Akteuren durch die inhärenten Sicherheitsrisiken vernetzter elektronischer Informationssysteme mit ihrer Größe. Verwundbarkeit wirft jedoch die Frage nach der politischen Bemessung von Schaden auf. In Unternehmen oder privaten Haushalten lassen sich die Werte physischer Gegenstands und Daten bestimmen. Aber welche Kriterien soll die Politik anlegen, um einen Angriff von Terroristen auf ein Computernetzwerk mit einem Anschlag auf eine U-Bahn zu vergleichen? Für eine Reaktion und deren Verhältnismäßigkeit werden solche Kriterien jedoch gebraucht.

Momentan bauen viele Staaten „offensive Cyberwar-Programme auf",[25] deren mittelbarer Zweck es auch ist, den Stellenwert anderer Akteure im Cyber-Space herabzusetzen und das Gewaltmonopol stärker in Richtung des Staates zu verlagern. Gruppen von spezialisierten Individuen, wie Anonymous, die es wiederum weniger spezialisierten Individuen ermöglichen, an Hacker-Angriffen teilzunehmen, machen aber deutlich, dass sich das Machtpendel im Cyber-Space nicht mehr zu Gunsten der Staaten verschieben wird. Selbst ohne viel technisches Wissen kann jemand als Blogger oder Twitterer, wie während der arabischen Facebook Revolutionen, zum Akteur im Cyber-Space werden, der die Stellung eines Staates unmittelbar, mittelbar aber aller Staaten untergräbt. Für die Staaten geht es daher nicht mehr um den Erhalt von Souveränität oder Gewaltmonopol, sondern um den Erhalt eigener Handlungsfähigkeit im Cyber-Space als „dem fünften Schlachtfeld neben Land, Luft, Meer und Weltraum".[26] Natürlich werden die Militärs mächtiger Staaten aufgrund ihrer bereiten Ressourcenbasis über starke Mittel verfügen, jedoch aufgrund von Beschränkungen, wie Datenschutz, politischer Interessen, öffentlichem Druck und möglicher Reaktionen anderer Staaten, nicht in der Lage sein, diese in dem Maße einzusetzen, dass sich das staatliche Gewaltmonopol wieder herstellen ließe.

Während bis hier primär von Staaten und nicht-staatlichen Akteuren im Allgemeinen die Rede war, darf man die wachsende Rolle der Cyber-Sicherheitsindustrie nicht vernachlässigen. Je mehr die Bedeutung des Cyber-Space wächst, desto wichtiger wird diese Industrie und desto größer werden ihre Profitmöglichkeiten. Mahnende Stimmen warnen bereits vor einem „militärisch-kybernetische[n] Komplex".[27]

23 Ebd., S. 89.

24 Lord, K. & Sharp, T. (2011). America's Cyber Future, S. 20.

25 Gaycken, S. (2011). Krieg der Rechner, S. 92.

26 Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. (2010). On Cyber Warfare, S. 6. http://www.chathamhouse.org.uk/files/17817_r1110_cyberwarfare.pdf (25.06.2011).

27 Hersh, S. (2011). Cyberwar: Die neue Front. http://www.blaetter.de/archiv/jahrgaenge/2011/

Unabhängig von der Frage, wie berechtigt solche Warnungen sind, ist allein ihr Aufkommen Beweis dafür, dass die Stellung des Staates im Cyber-Space weiter erodiert. Sicherheitspolitik wird für den Staat durch die diffusen Akteure, die Manipulierbarkeit aller Ereignisse und die Asymmetrie der Vorgänge zu einer kaum erfüllbaren Aufgabe.

Der Stellenwert des Netzes und Herausforderungen

Im Jahr 2010 überschritt die Zahl der Internetznutzer die Marke zwei Milliarden, die Zahl der Handynutzer die der fünf Milliarden.[28] Eine Änderung dieses Trends ist nicht zu erwarten. Stattdessen wird nach der offenbarten Macht des Internets während der arabischen Revolutionen allein das Bevölkerungs- und Wirtschaftswachstum der BRICSAM-Staaten[29] dafür sorgen, dass die Zahl der Internetznutzer weiter wächst und damit der Stellenwert des Cyber-Space samt seiner Sicherheit zunimmt.

Über die Wahrscheinlichkeit zwischenstaatlicher Cyber-Kriege lässt sich heute nur spekulieren, zumal sich die technischen Entwicklungen innerhalb staatlicher Stellen dem Beobachter durch die hohe Geheimhaltung verschließen. Wahrscheinlich ist, dass solche Cyber-Kriege, im Verborgenen ablaufen, weil offene Cyber-Kriege zwischen Staaten zwangsläufig Fortführung in der realen Welt finden würden. An dieser Stelle greifen aber die bestehenden Mittel konventioneller und nuklearer Abschreckung unter Staaten.

Spionage und Kriminalität sind bereits Alltagsphänomene im Cyber-Space. Dazu wird sich der Cyber-Aktivismus, wie man ihn während der arabischen Revolutionen, bei VroniPlag oder Anonymous sehen konnte, als Dauerphänomen hinzugesellen. Je mehr Menschen das Internet nutzen, desto mehr werden sich soziales und politisches Leben dorthin verlagern. Sicherheitspolitiker müssen also in Zukunft damit rechnen, sich einer blitzartig mobilisierten Maße gegenüber zu sehen, die bestimmte Ansprüche oder Kritik, vielleicht auch Lob äußert, auf die aber gerade in Demokratien reagiert werden muss, was den Ereignisdruck für die Politik erhöht.

Politik ohne Initiative: Was tun?

Wie schon dargestellt, kann staatliche Sicherheitspolitik ihrer Schutzaufgabe kaum noch gerecht werden. So gilt es, sich beim Schutz einen Schwerpunkt auf die Sicherheit kritischer Infrastruktur zu legen. Allerdings befindet sich die Infrastruktur (z. B. Strom-/Kommunikationsnetze) in privater Hand, was dem Staat wenig aktiven Gestaltungsspielraum gibt. Der mangende Gestaltungsspielraum des Staates ist dessen Schwäche, denn dadurch hat die Politik die Möglichkeit zur Initiative verloren. Handlungsinstrumente und Handlungsraum besitzt der Staat nach wie vor, aber sein Gestaltungsinstrument ist das Gesetzgebungsverfahren. Allerdings ist das Ereignistempo im Cyber-Space derart hoch, dass ein Gesetz durch die Fortentwicklung der Technik überholt ist, wenn es zur Anwendung kommt. Anstatt ihr neues sicherheitspolitisches Umfeld zu *regieren*, werden Staaten wie in der Vergangenheit bereits nur darauf *reagieren*.

Dazu gehört auch die Kluft zwischen jüngeren und älteren Politikern. Was manchem Jungpolitiker an politischer Erfahrung fehlt, fehlt manchem altgedienten Politikern aufgrund ihrer anderen Sozia-

januar/ cyberwar-die-neue-front (25.06.2011).

28 Lord, K. & Sharp, T. (2011). America's Cyber Future, S. 21.

29 Brasilien, Russland, Indien, China, Südafrika, ASEAN und Mexiko.

lisation an Sachverstand über den Cyber-Space. Stattdessen sind es gerade junge Akteure außerhalb der Politik, wie Mark Zuckerberg gewesen, die den Cyber-Space entscheidend mitgestaltet haben. Für einen sichereren Cyber-Space bedarf es intensivierter Kooperation zwischen Politik und Wirtschaft, wobei Vertrauensdilemma und rechtliche Fragen beim gegenseitigen Einblick in die IT-Systeme zuerst gelöst werden müssen. Außerdem bleibt innerhalb der staatlichen Apparate bei der Kommunikation von unten nach oben viel Fachwissen auf der Strecke. Während auf der Arbeitsebene viel technisches Fachwissen über einen Sachverhalt und dessen Lösung existiert, wird der Anteil an technischem Inhalt auf dem Weg nach oben durch die politische Hierarchie mit jeder Stufe reduziert. Stattdessen wird der betreffende Sachverhalt zunehmend politisiert, etwa von Beratern, denen ebenfalls technischer Sachverstand fehlen mag, so dass der politische Entscheidungsträger eine Beratungsvorlage erhält, deren Lösungsvorschläge, meistens wesentlich weniger der technisch sinnhaften Lösung gemeinsam haben. Die diversen aufeinanderprallenden Interessen innerhalb der politischen Hierarchien sind hier ein zusätzlicher, die Sache verkomplizierender Faktor, der in pluralistischen Systemen auch nicht eliminierbar ist.

Für Demokratien stellt sich außerdem das Problem parlamentarischer Kontrolle des Handelns der Exekutive im Cyber-Space. Diese Kontrollverfahren sind langwierig und alleine durch die Masse der beteiligten Akteure kompliziert. Automatisierte elektronische Verfahren, die unter dem hohen Ereignisdruck des Cyber-Space arbeiten entziehen sich weitgehend parlamentarischer Kontrolle, zumal das Herrschaftswissen über diese Prozesse bei Spezialisten aus den Bürokratien liegt und für den gewöhnlichen Parlamentarier kaum verständlich ist. Demokratien sollten daher darauf achten, die wissenschaftlichen Dienste ihrer Parlamente mit genug Kompetenz auszustatten, um diese Wissenslücken schließen zu können.

Informationen sensibelster Natur sind in der Cyber-Zukunft nur dadurch zu schützen, dass sie entweder in geschlossenen Systemen ohne Internetanschluss gespeichert sind oder gar nicht erst in elektronischer Form vorliegen. Ansonsten gilt es für Politik und Gesellschaft einfach damit zu leben, dass es im Cyber-Space keine Gewissheit der eigenen Unversehrtheit gibt. Wem dies bewusst ist, der kann sich darauf einstellen. Nichtsdestotrotz gilt es vor allem die positiven Seiten von mehr Cyber-Space zu sehen. Der Fall der arabischen Diktaturen wäre ohne das Internet nicht möglich gewesen. Eine durch das Netz entstehende und zusammenwachsende globale transnationale Zivil- oder Facebook-Gesellschaft macht reale Kriege und Konflikte durch die Masse entstandener zwischenmenschlicher Bindungen unwahrscheinlicher.

Die Rolle der Politik liegt nicht in der Herstellung von Sicherheit. Politiker müssen Cyber-Politik als Risikomanagement verstehen. Es gilt die Risiken für den Souverän in Grenzen zu halten und den Cyber-Space sicherer zu machen oder mindestens ein Ausbreiten der Unsicherheit einzugrenzen. Ein ehrliches Fazit muss allerdings lauten, dass auch eine Politik staatlicher Cyber-Sicherheitsrisikominimierung aufgrund der systembedingten Langsamkeit politischer Entscheidungsprozesse geringe Erfolgsaussichten hat. Jeder potenzielle „Gegner“ kann und wird Debatten und Gesetzgebungsverfahren mitverfolgen, weiß also was auf ihn zukommt und kann sich entsprechend vorbereiten. Tritt das entsprechende Gesetz also in Kraft, haben sich

genau diejenigen, gegen die es gerichtet ist, bereits seiner Wirkung entzogen.

Internationale Lösungen

Als Ideen zur Risikominimierung werden ein Non-Proliferationsvertrag für Cyber-Waffen und eine internationale Cyber-Sicherheitsagentur genannt. Hier muss allerdings festgehalten werden, dass beide Ideen in ihrer Umsetzung unrealistisch sind.

Non-Proliferationspolitik per Vertrag war im Bereich der kinetischen Massenvernichtungswaffen bereits nicht erfolgreich. Trotz aller internationalen Regime wurden Israel, Pakistan und Nordkorea Nuklearmächte. Iran wird folgen. Für einen Cyber-Nonproliferationsvertrag müssten sich die Regierungen von 193 Staaten einig werden, was eine Einigung über ein solch sensibles Thema, speziell mit Blick auf die USA, Russland und China, zu einem unrealistischen Ziel macht. Als wahrscheinlicher kann gelten, dass keiner der drei Staaten ein Interesse an einem derartigen Abkommen hat, da man sich in seinen militärischen Cyber-Aktivitäten nicht wird einschränken lassen wollen. Als Argumente für einen solchen Vertrag ohne diese drei Staaten oder zwischen einer begrenzten Anzahl von Staaten lassen sich theoretisch die politische Signalwirkung und das Entstehen politischen Drucks ausmachen. Beide Argumente treffen aber praktisch nicht zu, da die Aktivitäten rund um Cyber-Waffen so geheim ablaufen und Kerninteressen der Staaten betreffen, dass sie sich sowohl der Signalwirkung wie dem Druck entziehen. Darüber hinaus müsste ein Non-Proliferationsvertrag für Cyber-Waffen nicht nur von 193 Regierungen unterzeichnet, sondern auch von allen Staaten ratifiziert werden. Angesichts der Masse an involvierten Akteuren innerhalb der Staaten ist die Ratifizierung ebenfalls unrealistisch. Weiterhin käme ein solcher Vertrag nicht ohne die Beteiligung nicht-staatlicher Akteure aus. Konsens zwischen 193 Staaten und einer Unzahl an nicht-staatlichen Akteuren wird aufgrund der Masse divergierender Interessen nicht erzielbar sein. Dazu müssten sich alle Beteiligten auf eine Definition von Cyber-Waffen einigen, was wiederrum die Freigabe eigenen Wissens bedingen würde. Die Bereitschaft anderen Akteuren auf diese Weise Einblick in die eigenen (Un-) Fähigkeiten zu gewähren, kann überall als gering eingeschätzt werden.

Was für den Non-Proliferationsvertrag gilt, gilt in ähnlicher Weise auch für die Idee der Cyber-Sicherheitsagentur. Damit diese Agentur handlungsfähig wäre, müsste sie von den Beteiligten mit Wissen ausgestattet werden. Kaum ein Akteur wird bereit sein, sensibles Wissen zur Verfügung zu stellen. Vorher müssten sich die Beteiligten außerdem einig geworden sein, welche Posten in der Agentur von welchem Akteur besetzt werden. Es bedürfte einer Finanzierung, die immer für politischen Streit sorgt. Weitere schwer lösbare Streitpunkte wären die geographische Ansiedlung der Agentur und ihre Kontrolle. Man stelle sich die Reaktionen in den USA auf den Vorschlag vor, die Agentur in Moskau anzusiedeln und einen Chinesen als Leiter zu ernennen.

Ziele deutscher Cyber-Außenpolitik

Mit einer Abteilung für Cyber-Außenpolitik innerhalb des Auswärtigen Amtes[30] hat die Bundesregierung bereits eine Grundlage dafür gelegt, das Thema stärker auf diese Agenda der Berliner Republik zu setzen. Angesichts der analysierten Entwicklungen kann dies nur begrüßt werden. Allerdings bedarf es nun Vorgaben und Arbeitsaufträ-

30 Auswärtiges Amt (2011). Organisationsplan, S. 2. http://www.auswaertiges-amt.de/cae/servlet/contentblob/373560/publicationFile/156967/Organisationsplan.pdf (17.08.2011).

ge seitens der politischen Führung, welche Cyber-Außenpolitik oder was im Rahmen von Cyber-Außenpolitik durch diese Abteilung oder andere Stellen umgesetzt werden soll. Auch wenn die Ideen von Proliferationsvertrag und Agentur unrealistisch sind, sollte Deutschland seinen Einfluss innerhalb der VN nutzen, um dieses dort bisher nicht präsente Thema auf der VN-Bühne einzuführen. Eine unverbindliche Resolution in der Generalversammlung wäre ein Anfang, da es für die internationale Politik von Vorteil wäre, eine Beratungsgrundlage zu haben, würde international eine Cyber-Krise ausbrechen.

Die beiden anderen Schwerpunkte deutscher Cyber-Außenpolitik sollten in Brüssel liegen. Innerhalb der EU gilt es weniger, für Risikomanagement zu sorgen, als vielmehr die politische Kontrolle über die Datenspeicherungs- und Überwachungsprojekte zu intensivieren. Auf der militärischen Seite, sollte sich die Bundesregierung für intensive Kooperation zwischen den NATO-Staaten in der Cyber-Sicherheit einrichten. Ganz gleich, was der einzelne Beobachter oder Politiker von der Rolle des Militärs im Cyber-Space halten mag, die NATO ist die einzige Möglichkeit von Deutschen wie Europäern auf die militärische Cyber-Agenda der USA Einfluss nehmen zu können.

Zu deutscher Cyber-Außenpolitik gehört allerdings auch eine ehrliche Sprache zu Hause. Der Bevölkerung sind die Grenzen politischen Handelns deutlich zu machen. Gesellschaft und Wirtschaft müssen durch die Politik stärker sensibilisiert werden, ihr eigenes Risikomanagement voranzutreiben, denn die Politik wird dies im Cyber-Space nie leisten können.

Angaben zum Autor

*Felix F. Seidler, M.A. arbeitet als Redakteur für die Atlantische Initiative in Berlin und bloggt auf seinem eigenen Blog Seidlers Sicherheitspolitik zur verschiedenen sicherheitspolitischen Themen.