**Zeitschrift:** Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie SAK = Criminologie / Groupe Suisse de Criminologie GSC = Criminologia / Gruppo Svizzero di Criminologia GSC

**Herausgeber:** Schweizerische Arbeitsgruppe für Kriminologie

**Band:** 30 (2012)

**Artikel:** Cyber(Un)Sicherheit : Gegenwart und Zukunft der digitalen Bedrohung

**Autor:** Dunn Cavelty, Myriam

**DOI:** https://doi.org/10.5169/seals-1051470

# Cyber(Un)Sicherheit: Gegenwart und Zukunft der digitalen Bedrohung

MYRIAM DUNN CAVELTY
Dr., Center for Security Studies, ETH Zürich

**Inhaltsverzeichnis**



## Zusammenfassung

Dieser Beitrag führt in die unsichere Welt von Computernetzwerken ein und beschreibt, welche (unsichtbaren) Gefahren sie mit sich bringt. Es wird eine Unterteilung in verschiedene Cyberphänomene vorgenommen und deren gegenwärtigen und zukünftigen Ausprägungen einzeln diskutiert. Abschliessend werden die wichtigsten politischen Fragen erörtert, die sich durch den Schutz des Cyberraums ergeben.

# 1. Einleitung

Gegenwärtig vergeht kaum eine Woche, in der nicht ein Cybervorfall für Schlagzeilen sorgt. Noch vor kurzem ein Nischenthema für Militärstrategen und wenige Fachexperten, ist die digitale Bedrohung im Laufe des letzten Jahres zu einem Lieblingsthema der Medien avanciert und heute in (fast) aller Munde. Dabei ist die Thematik nicht nur für jeden einzelnen Computerbenutzer relevanter geworden, sondern auch für viele Staaten, die die Cyberbedrohung als eine Hauptgefahr für die nationale Sicherheit sehen und die in den letzten Jahren spezifische Cybersicherheitsstrategien entworfen oder überarbeitet haben.[1]

Heutzutage weist jeder politische, wirtschaftliche und militärische Konflikt eine Cyber-Komponente auf. Mit Hilfe von Computern werden politische und wirtschaftliche Spionage betrieben. Die Zahl der kriminellen Angriffe nimmt zu und mit ihr der finanzielle Schaden. Auch das organisierte Verbrechen hat sich längst im virtuellen Raum breit gemacht. Kopfzerbrechen bereiten Staat und Wirtschaft dabei zum einen die steigende Verwundbarkeit – hauptsächlich aufgrund der zunehmenden Verschmelzung sensibler staatlicher wie unternehmenseigener Infrastrukturen mit dem Internet – zum anderen die zu beobachtende Professionalisierung der „Malware-Branche“[2], mit immer komplexeren, raffinierteren, schwieriger abzuwenden und höheren Schaden anrichtenden Angriffen[3].

Die Cyber-Bedrohung birgt alles in sich, was bei Menschen maximale Angst auslöst: Ein Angriff kommt sozusagen aus dem Nichts, kann jederzeit und überall erfolgen, kann jeden treffen, kann praktisch nicht aufgehalten werden und birgt ultimativ die Gefahr für das Ende der menschlichen Zivilisation in sich. Nicht umsonst dreht sich die Cyber-Debatte also häufig um schwerwiegende Folgen von Ausfällen in der Informations- und Kommunikationstechnologie (IKT). Natürlich kann es in einer hoch technisierten Welt wie der unseren unangenehme, gar fatale Folgen

---

1 Beispiele dafür sind zum Beispiel: Deutschland, Frankreich, Grossbritannien, Indien, die Niederlande, die Vereinigten Staaten, und die Schweiz.

2 Malware ist ein Kofferwort aus den Worten "malicious" (böswillig) und "Software", auf Deutsch auch Schadprogramme genannt. Dazu gehören Viren und Würmer, also Computerprogramme, die funktionsfähige Kopien von sich selbst erstellen oder Trojanische Pferde, die, häufig getarnt als gutartige Anwendungen, im Hintergrund eine andere, verborgene Funktion ausführen.

3 Melde- und Analysestelle Informationssicherung (MELANI) (Hg.): Informationssicherung – Lage in der Schweiz und International. Halbjahresbericht 2010 (Juli – Dezember), Informatikstrategieorgan Bund: Bern 2011.

haben, wenn Computer aufgrund von Fehlern ausfallen oder von Übeltätern gezielt manipuliert werden. Doch obwohl die Möglichkeit einer eigentlichen *Super*katastrophe trotz einer verschwinden kleinen Wahrscheinlichkeit nicht vollständig ausgeschlossen werden kann, ist es bezeichnend, dass es in der gesamten Computer-Geschichte noch nie einen wirklich schwerwiegenden Vorfall von grossem Ausmass und mit langfristigen Folgen gegeben hat.

Wie denn ist die gegenwärtige Bedrohungslage einzuschätzen? Und wie entwickelt sie sich (wahrscheinlich) in der Zukunft? Dieses Kapitel widmet sich diesen Fragen. In einem ersten Unterkapitel wird Kapitel die Ausgangslage skizziert. In einem zweiten wird eine Unterteilung in verschiedene Cyberphänomene vorgenommen, deren Ausprägungen einzeln diskutiert werden. Im dritten Unterkapitel geht es um die wichtigsten politischen Fragen, die sich durch den Schutz des Cyberraums ergeben.

## 2. Allumfassende Verwundbarkeit als Ausgangslage

In den 1980ern wurde die Cybergefahr noch als vor allem Regierungsnetzwerke betreffend angesehen und die Debatte war auf Cyberspionage fixiert. Erst in den späteren 1990ern ist eine qualitative Veränderung der Bedrohungswahrnehmung zu beobachten. Vermehrt wurden in (amerikanischen) Dokumenten eine Verknüpfung zwischen Computern (oder Informationsinfrastrukturen) und sogenannt kritischen Infrastrukturen gemacht.[4]

Die Ausgangslage sieht demnach wie folgt aus: Die moderne technologisierte Gesellschaft ist auf das zuverlässige Funktionieren von *Infrastrukturen* angewiesen. Unter dem Begriff Infrastrukturen – bestehend aus den beiden Wörtern Infra („unterhalb") und Struktur („Gefüge, Bau, Aufbau") – versteht man Anlagen, Einrichtungen, Organisationen, aber auch Prozesse, Produkte, Dienstleistungen und Informationsflüsse, die den „Unterbau" für das reibungslose Funktionieren der Gesellschaft, der Wirtschaft und des Staates bilden.[5] Als kritisch werden jene Infrastrukturen bezeichnet, die bei einem Ausfall zu gravierenden politischen oder wirt-

[4] Dunn Cavelty, Myriam: Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate, Journal of Information Technology and Politics, Jg. 4, Heft 1, 2007, S. 19–36.

[5] President's Commission on Critical Infrastructure Protection: Critical Foundations: Protecting America's Infrastructures, Washington, DC: US Government Printing Office 1997.

schaftlichen Schäden führen können. In diese Kategorie fallen gemeinhin die Energieversorgung, die Kommunikation, das Gesundheitswesen, der Verkehr oder die öffentliche Sicherheit.[6]

So wichtig sie sind, so verletzlich sind sie: Zum einen bilden *Informations*infrastrukturen, die als inhärent unsicher gelten, häufig die Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen. Diese Debatte bedeutend mitgeprägt hat das US Militär, das in den frühen 1990er Jahren verstärkt über asymmetrische Bedrohungen nachzudenken begann. Es schien unumgänglich, dass zukünftige Gegner der absolut überlegenen militärischen Macht nur noch asymmetrisch begegnen konnten.[7] Die damals in Schwung kommende „Informationsrevolution" schien diese Möglichkeit noch zu verstärken. In den Augen von Sicherheitsexperten führte sie dazu, dass die Gesellschaft von einer Vielfalt von nationalen und internationalen Informationsinfrastrukturen abhängig – und deshalb verwundbar – wurde. Nicht nur gelten Informationsinfrastrukturen aufgrund technischer Unzulänglichkeiten als sehr unsicher, auch werden sie als besonders anfällig für asymmetrische Massnahmen seitens staatlicher und nicht-staatlicher Organisationen oder Einzeltäter angesehen, denn diese können durch die Nutzung weiterverbreiteter und kostengünstiger digitaler Angriffsmöglichkeiten maximalen Schaden anrichten.

Die Kommerzialisierung des Internets in den 1990er Jahren führte noch zu einer Verstärkung des Sicherheitsdefizits. Es gibt mehrere marktbedingte Hindernisse für Informationssicherheit: Sicherheit ergibt keine direkt sichtbaren Renditen. Harter Konkurrenzkampf und sehr schnelle Innovationszyklen von IT-Systemen sind hinderlich für die Einführung von Sicherheitsmaßnahmen, denn sie wirklich sicher zu machen, dauert häufig länger als die Entwicklung der IT-Nachfolgegeneration selbst, so dass der erstrebte Sicherheitsstandard nie erreicht wird. Zudem haben Sicherheitsstandards oft einen negativen Effekt auf die Funktionalität und Benutzerfreundlichkeit.[8]

---

6 Dunn Cavelty, Myriam/ Kristensen, Kristian Soby: Introduction: Securing the Homeland – Critical Infrastructure, Risk, and (In)Security, in Dies. (Hg), The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation, London: Routledge 2008, S. 1–14.

7 Pollard, Neal A.: Indications and Warning of Infrastructure Attack, in: Nicander, Lars/Ranstorp, Magnus (Hg.), Terrorism in the Information Age: New Frontiers?, Stockholm: National Defence College 2004, S. 43.

8 Andersson, Ross: Why Information Security is Hard: An Economic Perspective. In: IEEE Computer Society (Hg.): Proceedings of the 17th Annual Computer Security Applications Conference, Washington, 2001, S. 358–365.

## 3. Cyber(Un)Sicherheits-Kategorien und Trends

Die Cybervorfälle der letzten Jahre, und die mediale Aufmerksamkeit, die sie erhalten haben, haben den Anschein erweckt, dass wir mit mehr, immer besser organisierten und ganz allgemein kostspieligeren Vorfällen konfrontiert werden. Kurzum, die Gefahr scheint zu wachsen und zwar so schnell und stark, dass sofortige zusätzliche Anstrengungen notwendig sind. Interessant an dieser Gefahrenperzeption ist, dass wirklich stichhaltige Beweise zum Beispiel in Form von repräsentativen Daten fehlen[9]; so dass wir es weniger mit einem objektiv messbaren Anstieg der Bedrohung zu tun haben, als vielmehr mit einem subjektiven, kollektiven Gefühl der steigenden Unsicherheit. Gerade deshalb besteht die latente Gefahr, dass es zu einer undifferenzierten Sichtweise kommt.

Die informierte Diskussion über die Cybergefahr bedarf daher einer gewissen Systematisierung und Kategorisierung, die klare Aussagen über die gegenwärtige Gefahrenlage erlaubt und einen fundierten Blick in die Zukunft ermöglicht. Die eigentliche Herausforderung besteht darin, eine saubere Unterscheidung vorzunehmen zwischen solchen Problemen, die von hoher Dringlichkeit sind, weil ihre Konsequenzen den Staat per se oder eine zahlenmässig grosse Gruppe von Akteuren substantiell bedrohen und deshalb den Einsatz aussergewöhnlicher Mittel erfordern bzw. rechtfertigen; und zwischen solchen, die, auch wenn sie durchaus bedeutsam sind, mit den „normalen" ordnungspolitischen Instrumenten gelöst werden können oder nicht einmal die besondere Aufmerksamkeit des Staates bedürfen.

Eine dafür geeignete Kategorisierung von Cyberattacken nach Urhebern und deren Intentionen ist in der Praxis quasi unmöglich. Gut gemachte Angriffe sind unmöglich einem exakten Ursprung zuzuordnen. Das nennt man Attributionsproblem. Es umfasst zwei Teilaspekte: die personale Nicht-Attribution und die motivationale Nicht-Attribution. Der erste Ausdruck bezieht sich auf die Unmöglichkeit, eine Person mit Sicherheit für den Angriff verantwortlich zu machen bzw. diejenigen Personen zu

---

[9] Nicht, dass es an Statistiken und Trendreports fehlen würde; deren Validität und Reliabilität muss jedoch stark hinterfragt warden (siehe z.B. Guillot, Alexis/Kennedy, Sue: Information Security Surveys: A Review of the Methodologies, Critics and a Pragmatic Approach to their Purposes and Usage. In: Proceedings of 5th Australian Information Security Management Conference. Edith Cowan University, Perth, 2007 (http://ro.ecu.edu.au/ism/25/); Sommer, Peter/Brown, Ian: Reducing Systemic Cyber Security Risk. Report of the OECD's International Futures Project, IFP/WKP/FGS(2011)3. Paris, 2011.

finden, die ein Schadprogramm programmiert haben. Der zweite bezieht sich auf die Unmöglichkeit, die Absicht eines Angreifers zu eruieren.[10] Wenig erstaunlich: Das Attributionsproblem von Cyberattacken ist eines der Hauptthemen in der Cybersicherheitsdebatte, weil es die Logik der (militärischen und strafrechtlichen) Abschreckung fast gänzlich ausser Kraft setzt.

Trotz dieser praktischen Unmöglichkeit ist eine solche Kategorisierung jedoch theoretisch und konzeptionell wichtig: denn erst sie ermöglicht eine Veranschaulichung der Problematik. Die Unterscheidung nach Urhebern und deren Intentionen lässt das Bild einer Cybereskalationsleiter entstehen: je weiter oben auf der Leiter man sich befindet, desto grösser ist der mögliche Schaden. In den nachfolgenden Unterkapiteln werden sechs sich voneinander unterscheidende Cyberphänomene beschrieben. Wir schauen uns die Häufigkeit ihres Auftretens an, die neusten Entwicklungen in den jeweiligen Kategorien und charakterisieren die Auswirkungen, die dieses Phänomen hat.

## 3.1 Hacktivismus bzw. Cybervandalismus

*Beschreibung*: Kofferwort aus „Hacking" und „Aktivismus". Virtuelle Veränderung oder Zerstörung von Inhalten, wie z.B. das Hacken von Webseiten oder das Ausschalten eines Servers durch Datenüberflutung (DDoS-Attacke); oder auch die Veröffentlichung von gestohlenen (sensiblen) Daten (und Blossstellung der Bestohlenen).

*Häufigkeit*: Hat sich spätestens nach Kosovo-Intervention von 1999 als Begleiterscheinung aller politischen oder wirtschaftlichen Konflikte etabliert[11] und ist beliebtes Mittel von Online-Aktivisten.

*Trend*: Die Aktionen von WikiLeaks und der Hackerkollektive Anonymous oder LulzSec haben dem Hacktivismus unlängst sehr viel Aufmerksamkeit beschert. WikiLeaks handeln unter der Hackermaxime „Informationen sollten frei sein" und rütteln an der Macht von Staaten, gewisse Informationen im Namen der nationalen Sicherheit unter Verschluss zu halten. Die Hackerkollektive zeichnen sich durch ihren kreativen Umgang mit „Anonymität" in einer Zeit, in der der „gläserne Mensch" dank

[10] Gaycken, Sandro: Cyberwar: Das Internet als Kriegsschauplatz. München, 2011, S. 80-90.

[11] Dunn, Myriam: Information Age Conflicts: A Study of the Information Revolution and a Changing International Operating Environment. Zurich Contributions to Security Policy and Conflict Analysis Nr. 64. Zurich, 2002.

Sozialen Netzwerken wie Facebook Hochkonjunktur hat; und durch die Art und Weise, wie sie die mangelnden Sicherheitsvorkehrungen von prominenten Zielen öffentlich anprangern.

*Auswirkungen*: Grundsätzlich geringe (primäre) Kosten. Der Reputationsschaden für die Betroffenen ist jedoch tendenziell hoch, insbesondere bei ungeschicktem Krisenmanagement und -kommunikation. Auch der psychologische Effekt ist hoch, da Hacktivismus-Vorfälle besonderen Anklang in der Presse finden und so das Gefühl entsteht, ein digitaler Einbruch jage den andern.

## 3.2 (Wirtschaftliche) Cyberkriminalität

*Beschreibung*: Umfasst die zwei Kategorien Computerkriminalität (Straftaten, die mit dem Computer als Tatmittel begangen werden) und Internetkriminalität (Straftaten, die mittels Internet begangen werden). Die genauen Strafbestände sind im Strafgesetzbuch festgehalten. Beispiele sind Betrug, Identitätsdiebstahl oder Nutzung des Internets als Tatwaffe.

*Häufigkeit*: Sehr häufig.

*Trend*: In den Anfängen des Computerzeitalters prägten Einzeltäter das Bild; heute sind vor allem gut organisierte Profis am Werk. Wie viele reale Unternehmen arbeiten sie rund um den Globus und verfügen über strategische und operative Visionen, funktionierende logistische Abläufe und gezielten Personaleinsatz.[12] Angriffe werden gezielter und die dafür verwendeten Schadprogramme ausgeklügelter. Allerdings warnen gewisse IT-Sicherheitsunternehmen davor, dieser Art von Attacken allzu viel Gewicht beizumessen, nur weil mehr über sie berichtet wird.[13] Nur etwa 3% aller Vorfälle waren im 2010 so ausgereift, dass sie unmöglich zu stoppen waren. Die grosse Mehrheit der Angriffe ist simpel und auf rasche Erfolge aus, d.h. sie richten sich vor allem gegen kleinere und mittlere Unternehmen, die wenig Geld für IT-Sicherheit ausgeben.[14] Diese Arten von Vorfällen neigen dazu, unter dem Radar der Medien und sogar der Strafverfolgung zu bleiben.

---

12 Panda Security: Panda Security Report: The Cyber-crime Black Market: Uncovered. Bilbao, 2010.

13 Verizon: 2010 Data Breach Investigations Report: A Study Conducted by the Verizon RISK Team in cooperation with the United States Secret Service. New York, 2010, S. 16.

14 Maillart, Thomas/Sornette, Didier: Heavy-Tailed Distribution of Cyber-Risks. In: The European Physical Journal B, Jg. 75, Heft 3, 2010, S. 357–364.

*Auswirkungen*: Die Datenerhebung ist ausserordentlich schwierig, nicht nur weil das Phänomen so vielfältig ist, sondern auch, weil viele Vorfälle gar nie gemeldet werden oder ganz unentdeckt bleiben. Die geschätzten Direktkosten gehen je nach Methode der Erhebung weit auseinander die meisten Berichte gehen von steigenden Kosten aus. Der Reputationsschaden ist theoretisch hoch, aber die Dunkelziffer ist es ebenso – viele Vorfälle werden nie publik. Der psychologische Effekt ist für die Wirtschaft sehr hoch.

## 3.3 Cyberspionage (politisch und wirtschaftlich)

*Beschreibung*: Bezeichnet das unautorisierte Herumschnüffeln in Netzwerken beziehungsweise das Stehlen von Daten aus diesen Netzwerken. Die Cyberspionage ist ein Strafbestand laut Strafgesetzbuch.

*Häufigkeit:* Wahrscheinlich häufig: Es gibt jedoch keine Klarheit darüber, wie gross das Problem wirklich ist oder welche Art von Daten gestohlen und danach auch verwertet werden. Ersten kann davon ausgegangen werden, dass die Mehrzahl von Vorfällen unentdeckt bleibt, zweitens ist es sehr schwierig, einen (digital) Datendiebstahl festzustellen.

*Trend:* In den letzten Jahren wird China häufig für systematische Cyberspionage auf höchster Stufe verantwortlich sei. Stichhaltige Beweise für die Schuld der chinesischen Regierung gibt es jedoch aufgrund der Attributionsproblematik nicht.[15]

*Auswirkungen:* Die Kosten sind unklar (wie bei der Cyberkriminalität), aber potentiell hoch. Das gleiche gilt für den Reputationsschaden. Psychologisch hat die Berichterstattung über Cyberspionage vor allem eine Wirkung in Regierungskreisen.

## 3.4 Cybersabotage

*Beschreibung*: Die absichtliche Störung eines wirtschaftlichen oder militärischen Ablaufs zur Erreichung eines bestimmten (oft politischen) Ziels mit Cybermitteln.[16]

[15] Deibert, Ronald/Rohozinski, Rafal: Tracking GhostNet: Investigating a Cyber Espionage Network. Toronto, 2009.

[16] Anmerkung: Ab Stufe 4 verschwinden die Grenzen zwischen den Phänomenen zusehend. Zudem wäre Cybersabotage ziemlich sicher das Ziel eines Cyberterrorangriffs

*Häufigkeit*: Bisher erst ein öffentlich bekannter Fall (Stuxnet).

*Trend*: Stuxnet ist ein Computerwurm, der im Sommer 2010 zum ersten Mal Schlagzeilen machte. Stuxnet verhält sich anders als üblicherweise für Cyberkriminalität eingesetzte Schadprogramme. Es stiehlt keine Informationen, es verbirgt sich nicht auf Computern, um sie später für DDoS-Attacken oder ähnliches fernzusteuern. Es verbreitet sich auch nicht wahllos weiter. Vielmehr verübt Stuxnet Sabotage: Konkret hat der Wurm gezielt Systeme angegriffen, die zur Steuerung und Überwachung industrieller Prozesse dienen. Berichten zufolge handelt es sich bei Stuxnet um ein sehr komplexes Programm: Es zu schreiben erfordert viel technisches Wissen, u.a. auch von industriellen Prozessen. Und es erfordert das Kennen der spezifischen Schwachstellen des angegriffenen Systems. Das Programmieren dürfte daher auch sehr teuer gewesen sein. Da auch das Kernkraftwerk Bushehr im Iran betroffen war und der Iran allgemein die höchste Infektionsrate aufweist, scheint der Schluss nahe, der Wurm sei gezielt zur Sabotage eben dieser Anlage angesetzt worden.[17]

*Auswirkungen*: Potentiell sehr gross, wenn kritische Infrastrukturen davon betroffen sind; im Falle von Stuxnet jedoch nicht sehr hoch. Die psychologischen Auswirkungen von Stuxnet hingegen waren enorm: die Entdeckung des Wurms war massgeblich daran beteiligt, dass so viele Staaten dringenden Handlungsgrund im Cyberbereich feststellten.

## 3.5 Cyberterrorismus

*Beschreibung*: Rechtswidrige Angriffe nichtstaatlicher Akteure gegen Computer, Netzwerke, und die darin gespeicherten Informationen, mit dem Ziel, eine Regierung (und/oder die Bevölkerung) einzuschüchtern oder zu spezifischen Handlungen zu zwingen. Ein Cyberangriff wird also nur dann als Cyberterror bezeichnet, wenn er in physischer Gewalt gegen Personen oder Sachen mündet oder zumindest so viel Schaden anrichtet, dass beträchtliche Angst entsteht.[18]

---

oder einer Cyberkriegshandlung. Ich halte dennoch an dieser Unterteilung fest, weil damit spezifische Trends aufgezeigt werden können.

17 Farwell, James/Rohozinski, Rafal: Stuxnet and the Future of Cyber War. In: Survival: Global Politics and Strategy, Jg. 53, Heft 1, 2011, S. 23–40.

18 Denning, Dorothy: Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: Arquilla, John/Ronfeldt, David (Hg.): Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, 2001, S. 239–288.

*Häufigkeit*: In der Praxis sind bisher keine Fälle von Cyberterrorismus bekannt. Der meistgenannte Grund dafür ist, dass eine wirklich schwerwiegende Attacke schlicht zu schwierig ist; und dass mit konventionellen Mitteln (z.B. Sprengstoff) viel billiger und einfacher eine grössere Wirkung erzielt werden kann.[19]

*Trend*: Seit der Entdeckung von Stuxnet ist das Wort praktisch vollständig aus der Debatte verschwunden. Neu dreht sie sich fast ausschliesslich um den Cyberkrieg.

*Auswirkung*: Real und psychologisch sehr gross, da Hauptziel kritische Infrastrukturen wären.

## 3.6 Cyberkrieg

*Beschreibung*: Kriegerische Auseinandersetzung im virtuellen Raum, vorwiegend mit Mitteln aus dem Bereich der Informationstechnik. Der Cyberkrieg umschreibt einen Teilbereich des Informationskriegs, ein breiteres Konzept, das auch elektronische Kriegsführung, Propaganda, etc. umfasst. Das Wort Cyberkrieg wird (vor allem) in der Presse jedoch auch sehr unsauber für alle Arten von Cybervorfälle mit politischem Charakter verwendet.

*Häufigkeit*: Einen reinen Cyberkrieg hat es noch nie gegeben. Kleinere Cybervorfälle sind jedoch Begleiterscheinungen von bewaffneten Konflikten (z.B. in der Form von Hacktivismus): und Aspekte des Informationskriegs – wie die elektronische Kriegsführung – sind nicht nur doktrinal festgeschrieben, sondern längst auch Realität. Streng genommen ist es falsch, sie Cyberkrieg zu nennen; aber dies ist eine sehr häufige Praxis.

*Trend*: Eine ganz neue Wendung hat die Debatte nach der Entdeckung von Stuxnet genommen. Die bereits oben beschriebenen Merkmale (Verhalten, Zweck und Kosten) legen in ihrer Kombination den Schluss nahe, dass ein (oder mehrere) Nationalstaat(en) involviert gewesen war. Falls aber ein Nationalstaat einen anderen Nationalstaat mit Hilfe eines Computerprogramms angegriffen und damit physischen Schaden verursacht hat, ist der Cyberkrieg für einige Experten nicht länger nur Theorie. Der „digitale Erstschlag" ist erfolgt,[20] Pandoras virtuelle Büchse offen – und Cy-

[19] Nicander, Lars/Ranstorp, Magnus: Terrorism in the Information Age – New Frontiers? Stockholm, 2004.

[20] Rieger, Frank: Trojaner „Stuxnet": der digitale Erstschlag ist erfolgt. In: FAZ.net v. 22.9, 2010.

berkrieg ist keine Kriegsform der Zukunft mehr, sondern Realität.[21] Auch wenn solche Schlüsse mit einem grossen Fragezeichen versehen werden müssen: Stuxnet hat die Cybersicherheitsdebatte nachhaltig verändert.

*Auswirkungen*: Real und psychologisch sehr gross, da Hauptziel kritische Infrastrukturen wären.

## 4. Wie Schutz gewährleisten?

Die Ausführungen im obigen Kapitel zeigen, dass sich Cybervorfälle bisher fast ausschliesslich auf den Stufen 1–3 abspielen. Die Phänomene auf Stufe 4, 5 und 6 sind äusserst selten oder sogar gänzlich Zukunftsmusik. Dennoch: Der virtuelle Raum ist heute bereits ein wichtiger Konfliktplatz unterhalb der Kriegsschwelle, auf dem sich Akteure jeglicher Couleur tummeln, sei es ganz offen oder eher klandestin, mit verschiedenen Motiven und unterschiedlichen Fähigkeiten. Es ist nicht anzunehmen, dass sich daran in Zukunft viel ändern wird. Im Gegenteil: Die Cyber-Dimension wird über fortschreitende Vernetzung noch substanziell an Wichtigkeit gewinnen – mit verschiedenen Konsequenzen für Politik, Wirtschaft und Gesellschaft.[22] Es ist also unumstritten, dass Abhängigkeiten bestehen und dass die „böse" Seite des Cyberspace etwas ist, mit dem sich die Politik in verschiedenen Varianten zu beschäftigen hat. Umstritten sind jedoch die politischen Schlüsse, die aus dieser Tatsache gezogen werden sollten, vor allem in Bezug auf die Details der Bedrohungslage und die Art und Intensität der Gegenmassnahmen, die von staatlicher Seite getroffen werden müssen.

Cybersicherheit ist ein typisches Querschnittsthema, das – wie im Fall der Terrorismusabwehr – der Kooperation zwischen den verschiedensten Akteuren mit teilweise sehr unterschiedlichen Kulturen bedarf. Dabei handelt es sich nicht nur um Behörden, sondern auch um Akteure aus der Wirtschaft und aus der Gesellschaft. Es stellt sich also die Frage, welche Rolle der Staat im Bereich der Cybersicherheit spielen soll, darf, muss und kann. Denn der Staat kann alleine unmöglich für die Erhöhung der Cybersicherheit sorgen. Cybersicherheit ist auch zu einem grossen Teil

---

21 Gross, Michael Josep: Stuxnet Worm: A Declaration of Cyber-War. In: Vanity Fair, April, 2011. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

22 Rueda-Sabater, Enrique/Derosby, Don/Johnston, Jenny/ Murphy, Nancy Murphy: The Evolving Internet: Driving Forces, Uncertainties, and Four Scenarios to 2025, Cisco/Global Business Network 2010.

Aufgabe jeder Privatperson und jeder Firma. Nicht nur ist die Industrie (und auch der Mittelstand) ganz besonders von Cyberkriminalität und -spionage betroffen; auch befinden sich die meisten kritischen Infrastrukturen in privater Hand, so dass der Staat deren Schutz vor Cyberattacken nicht einmal im Ansatz allein garantieren kann. Darüber hinaus beinhaltet die breite Palette an notwendigen Gegenmassnahmen viele Elemente, die ebenfalls nicht staatlich konzipiert oder umgesetzt werden können.

## 4.1 Zwei Spannungsfelder

Ein zufriedenstellendes Niveau an Cybersicherheit kann nur im Verbund zwischen Staat, Wirtschaft und Gesellschaft erreicht werden. Doch verfolgen die einzelnen Sektoren häufig unterschiedliche Interessen. Daraus entstehen zwei Spannungsfelder, in denen jede Cybersicherheitspolitik positioniert werden muss. Wo die Cybersicherheitspolitik auf diesen zwei Achsen verordnet wird und wohin sie sich hinbewegt, ist das Resultat komplexer Aushandlungsprozesse, die stark von einzelnen Ereignissen und damit zusammenhängenden Gefahrenperzeptionen abhängig sind.

Im ersten Spannungsfeld zwischen Staat und Wirtschaft gilt es, eine Politik zur Sicherung der kritischen Infrastrukturen zu formulieren, welche die negativen Konsequenzen der Liberalisierung, Privatisierung und Globalisierung aus Sicht der Sicherheitspolitik auffängt, ohne die positiven Effekte zu verhindern. Wie kann der Markt, der zudem mit dem Problem von Quasimonopolen konfrontiert ist, so reguliert werden, dass eine optimale Balance zwischen Sicherheit und Funktionalität entsteht? Wie können Anreize zu mehr Sicherheitsverpflichtung für Anbieter von Dienstleistungen geschaffen werden? Wie können die Nutzer dahingehend sensibilisiert werden, dass sie ein Mehr an Funktionalität nicht länger vor Sicherheitsdenken setzen? Wie können die (globalen) rechtlichen Rahmenbedingungen für Aktivitäten im virtuellen Raum angeglichen werden, um der Gefahr von "Schlupflöchern" und dem Vorrang von billigen Lösungen entgegenzuwirken? Wie kann Vertrauen zwischen Wirtschaft und Staat geschaffen werden?

Im zweiten Spannungsfeld zwischen Staat und Bürger gilt es, die richtige Balance zwischen mehr Sicherheit und Freiheit im digitalen Raum zu finden. Zusätzlich geforderte polizeiliche oder geheimdienstliche Befugnisse geraten dabei häufig in Konflikt mit Bürgerrechten, insbesondere dem Grundrecht auf informationelle Selbstbestimmung oder der Anonymität im Netz. Bei eingehender Beschäftigung mit Cybergefahren wird

gern vergessen, dass trotz der erhöhten Aufmerksamkeit und den Rufen nach mehr und besserem Schutz die Cybersicherheit nur eines von vielen komplexen, intersektoriellen Themen ist, denen sich der Staat heute zu widmen hat. Gleichzeitig ist der finanzielle „Leidensdruck", der durch bisherige Cybervorfälle entstanden ist, nicht hoch genug, um substanziell höhere Kosten und Einschnitte bei den Bürgerrechten akzeptabel zu machen.

## 4.2 Die Rolle des Staates

Im internationalen Vergleich zeigt sich, dass der Staat zwar eine wichtige, aber dennoch kleine Rolle in der Cybersicherheit spielt. Die Hauptaufgabe des Staates ist das Sichern der eigenen zivilen und vor allem auch militärischen Netzwerke gegen alle Formen von Cyberkonflikten mit technischen und anderen Mitteln. Auch hat der Staat die Aufgabe als Gesetzgeber, die nötigen rechtlichen Grundlagen zu schaffen oder anzupassen, um z.B. Cyberkriminalität in den unterschiedlichsten Formen zu bekämpfen. Da Akteure im Cyberspace meist international agieren, kommt auch der internationalen Dimension, insbesondere im Bereich der strafrechtlichen Zusammenarbeit, eine grosse Bedeutung zu. Ebenfalls grossgeschrieben wird das Thema „Sensibilisierung" der breiten Öffentlichkeit für Cyberfragen. Im Bereich der kritischen Infrastrukturen versuchen alle westlichen Staaten mit sogenannten öffentlich-privaten Partnerschaften für mehr Schutz und Resilienz – also der Widerstandsfähigkeit von Netzwerken – zu sorgen. Dabei handelt es sich mehrheitlich um die freiwillige Zusammenarbeit der Wirtschaft mit dem Staat, vor allem im Bereich des Informationsaustauschs.

Dabei sollte eines nicht vergessen werden: Auch in Zukunft wird keine Cybersicherheitsstrategie der Welt je dazu führen, dass der digitale Raum gefahrenfrei wird. Der Schutz kann noch so vielfältig und gut sein, Cyberkriminalität wird ein Problem bleiben, wie auch die Cyberspionage. Es lässt sich auch nicht ausschliessen, dass es zu grösseren Störungen in der kritischen Infrastruktur kommen wird, sei es aufgrund von spontanen technischen Störungen oder aufgrund menschlicher Eingriffe. Grundsätzlich ist umfassende Gewährleistung von Sicherheit angesichts der Vielfalt, der Komplexität und der Unvorhersehbarkeit moderner Risiken ohnehin längst nicht mehr möglich (wenn sie es je war). Gesellschaften müssen daher mit dieser Unsicherheit leben lernen und eine latente Toleranz in Bezug auf solche Ereignisse entwickeln. Dabei ist es Aufgabe der Politik,

diese Tatsache und die Grenzen staatlichen Handelns ehrlich zu kommunizieren, während sie gleichzeitig nach den besten Wegen sucht, die Sicherheit für die Gesamtgesellschaft nach Möglichkeiten zu maximieren.