Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur

Band: 98 (2018)

Heft: 1061

Artikel: Der Cyber-GAU, der so nicht kommt

Autor: Dunn Cavelty, Myriam

DOI: https://doi.org/10.5169/seals-816199

Der Cyber-GAU, der so nicht kommt

Das Narrativ potentieller Cyberkatastrophen hilft vor allem Staaten beim Aufbau entsprechender Kompetenzen. Das macht die Welt aber nicht sicherer.

von Myriam Dunn Cavelty

Eines Morgens fällt die Stromversorgung grossflächig aus. Bankautomaten geben kein Bargeld mehr heraus, Fahrstühle bleiben stecken, der Flugverkehr bricht zusammen. Die Ampeln spielen verrückt und auf den Strassen herrscht Chaos. Sicherheitskräfte verlieren die Kontrolle über Atomkraftwerke und Staudämme. Ganz Europa versinkt im apokalyptischen Chaos – Terroristen sind in unsere Computernetzwerke eingedrungen und bringen unsere Zivilisation zum Stillstand.

Übertrieben? Auf jeden Fall, denn eine solch grossangelegte Operation ist technisch nicht möglich. Und doch sind solche Schreckensszenarien seit vielen Jahren Teil des Cybersicherheitsdiskurses. Durch das hypothetisch drohende TEOTWAWKI *(The End of the World as We Know It)* steht nichts Geringeres auf dem Spiel als unsere gesamte Zivilisation. Nur: obwohl sie bereits seit über zwanzig Jahren erwartet wird, kommt und kommt die digitale Katastrophe einfach nicht. Und doch entfaltet sie eine unheimliche Wirkung, gerade weil sie ausbleibt: Gemäss den Prinzipien der Aufmerksamkeitsökonomie läuft sie weniger spektakulären Phänomenen den Rang ab und bindet knappe monetäre, intellektuelle und politische Ressourcen auf sich, obwohl sie nur in unserer Antizipation existiert.

Cyberunsicherheit – wie spektakulär ist sie?

Die Digitalisierung hat viele Aspekte unseres Lebens grundlegend verändert – viele davon zum Guten. Doch aufgrund der zunehmenden Abhängigkeit der Gesellschaft von Computern für den Datenaustausch und die Datenspeicherung entstehen neue Verwundbarkeiten für Staat, Wirtschaft und Gesellschaft. Daran wird sich in Zukunft nichts ändern, im Gegenteil: die Cyberunsicherheit dürfte aufgrund der fortschreitenden Vernetzung und Automatisierung substanziell zunehmen.

Aus Erfahrungen der letzten Jahre wissen wir: Der virtuelle Raum ist heute ein Konfliktplatz unterhalb der Kriegsschwelle, auf dem sich vermehrt auch staatliche Akteure tummeln, früher meist im Geheimen, heute zunehmend offen. In der Tat ist es für Staaten attraktiv, die technischen und politischen Effekte von Cyberoperationen in verschiedenen Kontexten auszutesten – denn die Kosten für die Angreifer sind relativ gering, während es für das Opfer schwierig und teuer ist, den Angreifer abzuwehren oder ihn eindeutig zu identifizieren und danach zu bestrafen.

Das prominenteste Beispiel für eine solche staatliche Aktion ist sicherlich Stuxnet, der Computerwurm, mit dem im Iran 2010 das Atomprogramm sabotiert und verlangsamt wurde; es gilt heute als bewiesen, dass dahinter die USA und Israel steckten, auch ohne offizielle Verlautbarung dieser Regierungen. Auch Erpressung kann unter Rückgriff auf Cybermittel erfolgen: so zum

In Kürze

Cyberkriminalität hat hohe gesellschaftliche Kosten. Doch die Gefahr einer eigentlichen Cyberkatastrophe wird drastisch überschätzt. Eine vernünftige Politik konzentriert sich deshalb auch in diesem Bereich auf das Abwägen von Interessen und Werten.

Gezielte Cyberoperationen mit grosser Wirkung können erwiesenermassen nur von staatlichen Akteuren mit genügend Ressourcen und nachrichtendienstlichen Fähigkeiten durchgeführt werden.

Je mehr Cyberkompetenzen der Staat hat, desto höher ist das Risiko, dass sie eines Tages missbraucht werden, auch gegen die eigenen Bürger. (lr)

«In der Cybersicherheitsdebatte wird die Technik selbst zur zielgerichteten Waffe.»

Myriam Dunn Cavelty

Myriam Dunn Cavelty, fotografiert von Suzanne Schwiertz.

Spione unter uns

Im Zweiten Weltkrieg wurde die Schweiz zur grössten Drehscheibe für ausländische Geheimdienste. Die Amerikaner legten hier den Grundstein für die spätere Macht der CIA. Noch heute ist die Diplomatenhochburg Genf ein Eldorado für das Geschäft mit Informationen.

Beispiel 2014, als (nordkoreanische) Hacker die Firma Sony dazu brachten, einen Film, in dem der Diktator Kim Jong Un umgebracht wird, nicht wie geplant in die Kinos zu bringen. Insbesondere im Zuge der hybriden Kriegsführung Russlands werden sie aber auch für Störungsaktionen und Destabilisierung des politischen Umfelds eingesetzt: so 2016, als russische Proxy-Akteure mit gestohlener Information aus dem Umfeld der Demokratischen Partei in den amerikanischen Wahlkampf eingriffen.

Doch auch wenn in den letzten Jahren viel über staatlich orchestrierte Cyberoperationen in den Medien berichtet wurde, sind sie sehr selten. Gezielte Cyberoperationen mit grosser Wirkung (z.B. Sabotage) können erwiesenermassen nur von staatlichen Akteuren mit genügend Ressourcen und nachrichtendienstlichen Fähigkeiten durchgeführt werden – allen voran von den USA. Darüber hinaus werden Cyberwaffen seit Stuxnet gerade aufgrund der Schwierigkeiten, strategisch kontrollierbare Effekte zu erzielen, und wegen des Bestrebens, das Risiko einer Eskalation klein zu halten, zurückhaltend eingesetzt. Die Grossmächte verwenden sie deshalb zum grössten Teil für Spionage. Wofür sie *nicht* eingesetzt werden, ist für die kriegsähnliche *Zerstörung,* wie wir es aus den Schreckensszenarien Hollywoods kennen.

Die allermeisten Cybervorfälle, denen *Firmen* und *Privatpersonen* tagtäglich ausgesetzt sind, sind in ihrer Alltäglichkeit sogar geradezu banal. Sie haben keinen Nachrichtenwert, so dass wir in den Medien nichts davon hören. Bill-Swap-Betrug, also der Austausch elektronischer Rechnungen im E-Mail-Konto, «Office 365»-Phishing-E-Mails, Sicherheitslücken im Zahlungsmanagementsystem «Smartvista» der Schweizer BPC Group, Datendiebstahl bei der Krankenkasse Groupe Mutuel..., das sind nur ein paar Beispiele von Cybervorfällen im letzten Jahr. Hinter diesen alltäglichen Cyberunsicherheiten stecken keine Staaten, sondern Kriminelle, davon manche sehr gut organisiert. Da viele Firmen Cybervorfälle weder den Behörden noch einer Versicherung melden, ist es sehr schwierig, den volkswirtschaftlichen Schaden wirklich zu berechnen, was zum Rückgriff auf Schätzungen führt, die naturgemäss sehr ungenau sind. Der Schweizerische Versicherungsverband SVV hat unlängst geschätzt, dass Cyberschäden und Massnahmen zum Schutz gegen Cyberrisiken in der Schweiz Kosten von 9,5 Milliarden Franken pro Jahr verursachen – eine erschreckend hohe Zahl, der aber zwecks Balance der jährliche Gewinn einer wachsenden Cybersicherheitsindustrie entgegengesetzt werden sollte.

Erzählte Katastrophen und ihre Wirkung

Ausser Zweifel steht: Cyberunsicherheit spielt sich auf vielen Ebenen gleichzeitig ab und die Auswirkungen sind real und vielfältig. Was es aber auch zu beachten gilt bei einer Einschätzung der Gefahrenlage, ist die Verzerrung unserer Wahrnehmung. Von wenigen Vorfällen hören wir viel – von den meisten hören wir nichts. Dass die Sichtbarkeit spektakulärer Vorfälle den weniger sichtbaren die Aufmerksamkeit stiehlt, ist wenig erstaunlich. Was das aber bedeutet und was diese Verzerrung politisch bewirken kann, sagen uns Ansätze aus der Risiko- und Sicherheitsforschung.

Die eingangs geschilderte Cyberkatastrophe mobilisiert immer noch viele Ängste, auch wenn die Realität der Cyberunsicherheit deutlich anders aussieht. Die Cyberkatastrophe existiert wie andere moderne Katastrophen – zum Beispiel der terroristische Einsatz von Massenvernichtungswaffen oder die Grosspandemie – in unserer Antizipation. Ganz unabhängig davon, wie die Wahrscheinlichkeit und das Ausmass solcher Ereignisse eingeschätzt werden, handelt es sich um «erzählte Katastrophen», Katastrophen, die ihre Wirkung in der Form von Narrationen entfalten. Solche Konstrukte bergen besondere Herausforderungen für Politik und Gesellschaft, weil sie in sich die Gefahr von verzerrten Gefahrenbildern bergen, die zu falschen Erwartungen und auch politischen Entscheiden und Investitionen führen können.

In der Gesellschaftstheorie blieb Technik lange ein relativ unbeachteter Faktor: Der Erfolg des Begriffs «Risikogesellschaft» änderte dies in den 1980er Jahren, als sich eine durch Ulrich Beck geprägte Denkrichtung für den Umgang moderner Gesellschaften mit unintendierten Folgen technologischen Fortschritts beziehungsweise der Antizipation möglicher Folgen von Technologie zu beschäftigen begann. Eine solche technopessimistische Betrachtungsweise spiegelt einen grundlegenden Wandel der Rolle von Technik im Rationalisierungsprozess wider: Von einem verlässlichen Mittel wird sie zum Unsicherheitsfaktor, indem sie Zwecke gefährdet und sogar destruktive Gefährdungen erst hervorbringt. In der Cybersicherheitsdebatte wird die Technik selbst zur zielgerichteten Waffe und durch die den Technologien eigene Unsicherheit zur Achillesferse moderner Gesellschaften.

Obwohl das Leben in westlichen Wohlstandsgesellschaften eigentlich immer sicherer wird, glaubt sich die Menschheit dort mit immer mehr und immer grösseren, immer umfassenderen Risiken konfrontiert. Im Zeitalter «grenzenloser» Risiken wird die Risikogesellschaft zur Weltrisikogesellschaft, einer Gesellschaft globaler Gefahreneinsichten. In diesem Fahrwasser ist die Cyberunsicherheit zum Sinnbild für die Verwundbarkeit der liberalen, offenen Gesellschaft und deren Schutzbedürfnis geworden. Sie ist Brennpunkt in einer politischen Debatte, in der schleichende Angst vor allgegenwärtiger Verwundbarkeit und eine unbestimmte Angst vor der Zukunft signifikante Merkmale sind. Aufgrund ihrer speziellen Position im gegenwärtigen sicherheitspolitischen Diskurs können die Cyberunsicherheit und damit zusammenhängende Katastrophennarrationen deshalb als Lehrstück für die Befindlichkeit moderner technologisierter Gesellschaften ganz allgemein betrachtet werden.

Risiken vergegenwärtigen einen Weltzustand, den es (noch) nicht gibt, und bedeuten so insgeheim immer auch die Antizipation der Katastrophe. Die Darstellung vom Risiko als antizipierter Katastrophe führt zur Frage, wer Risiken als solche definiert und bei wem die Macht der Definition ihrer Ausprägungen liegt. Im

«Im Falle der Cyberunsicherheit werden zwei zentrale Ängste miteinander verknüpft: die Angst vor der Technik und die Angst vor dem Terrorismus.»

Myriam Dunn Cavelty

Falle der erzählten Katastrophe produzieren Experten, politische Akteure und insbesondere auch die Medien Narrationen, in denen das Potenzielle mit der Wirklichkeit vermischt wird. Die ultimative Gefahr wird dadurch als immanent und real dargestellt. Wie Ulrich Beck einst bemerkte: «Politisch entscheidend ist letztlich nicht das Risiko, sondern seine Wahrnehmung. *What men fear to be real is real in its consequences* – Furcht schafft eine eigene Wirklichkeit.»

Wie bei der klassischen Gespenstergeschichte ist die Angst dann am grössten, wenn man eine Gefahr erwartet, aber nicht genau weiss, in welcher Form und wann sie auftreten wird. Cybersicherheitsdiskurse sind voll von Metaphern, bei denen es um die Auflösung von sicheren Zuständen durch neue, unberechenbare und auch unvorhersehbare Gefahren geht. Die Narrationen sind also geprägt von Macht- und Kontrollverlust; Nichtwissen an und für sich wird als Gefahr dargestellt, denn Nichtwissen führt zu Ungewissheit in bezug auf Zeitpunkt, Akteure, Ziele und Motivationen. Darüber hinaus werden im Falle der Cyberunsicherheit zwei zentrale Ängste miteinander verknüpft: die Angst vor der Technik und die Angst vor dem Terrorismus. Da beide vor allem mit Ungewissheit und Unsicherheit im Zusammenhang stehen, vermag die Kombination von Technik und Terrorismus besonders stark zu mobilisieren. Der Terrorismus – ganz gemäss terroristischem Kalkül – wird gefürchtet, weil er unverstehbar und unkontrollierbar erscheint und weil er das Sicherheitsgefühl eines jeden Menschen untergräbt. Informationstechnologie wiederum ist gefürchtet, weil ihr Einfluss auf das Individuum als komplex, abstrakt und arkan angesehen wird. Diese Angst hängt mit drohendem «Kontrollverlust» zusammen: Insbesondere im Zeitalter von weltumfassenden (Daten-)Netzwerken verliert der Mensch die Kontrolle über die Funktionen, die von Computern gesteuert werden. Die Cybersuperkatastrophe ist auch immer konzipiert als interdependente Katastrophe: Die Interdependenzen zwischen Systemen und Menschen und die Wahrscheinlichkeit von sogenannten Dominoeffekten, also Effekten, die ausserhalb unserer Kontrolle liegen, potenzieren die möglichen Auswirkungen um ein Vielfaches.

Angst und Mobilisierung

Die relative Banalität des Cyberalltags führt dazu, dass die hohe Wahrscheinlichkeit einer antizipierten Cyberkatastrophe im politischen Prozess bewiesen werden muss. Damit das funktioniert, wird das Risiko ihres Eintritts – immer unter Rückgriff auf Anekdoten und Ereignisse der Gegenwart als «near-misses» und zur Veranschaulichung «was hätte sein können» – als unmittelbar bevorstehend dargestellt. Der Logik dieser Mobilisierungsversuche folgend, werden dafür quasiapokalyptische Worst-Case-Szenarien verwendet, mit denen ein gigantisches Schadensausmass einhergeht. In Kombination führt das dazu, dass nicht mehr das eigentliche Risiko der Katastrophe die Hauptbedrohung darstellt, sondern vielmehr das Nichthandeln in der Gegenwart.

Erzählte Katastrophen führen so zu einer Reihe von unguten Nebeneffekten. Erstens nehmen sie im Gefahrendiskurs eine überproportional starke Stellung ein, auf Kosten längst realer und wichtigerer Probleme. Zweitens fungieren sie als sinnstiftende Referenzsysteme, vor deren Hintergrund gegenwärtige Entwicklungen und Ereignisse als apokalyptische Vorboten gelesen, gedeutet und politisch eingesetzt werden können. Sie werden zu Beweisen für die Notwendigkeit von ausserordentlichen (auch militärischen) Massnahmen und fungieren als Geldmaschine für eine diverse Industrie, die sich nicht vor der Angstmache scheut. Das Resultat sind Gesellschaften im Zustand der abwartenden Daueralarmierung, die sich fast obsessiv mit möglichen Schreckensbildern beschäftigen – und das, obwohl sie in privilegierten Teilen der Welt florieren, in denen die Sicherheit objektiv noch nie so gross war.

Cyberkatastrophen gewinnen aufgrund der suggerierten Dringlichkeit jeden Wettkampf mit anderen denkbaren Arten der

Prioritätensetzung, wie zum Beispiel der Cyberkriminalität. Auch reduziert die Ausrichtung auf Vorfälle mit gigantischem Schadensausmass den Beweiszwang, dass hinter solchen Schreckensszenarien nicht blosse Spekulationen, sondern auch tatsächlich zu erwartende Bedrohungen stecken. Und nicht zuletzt folgt dieser Art der Gefahrendarstellung gerne der reflexartige Ruf: «Der Staat macht nicht genug für die Cybersicherheit!», vielmals gehört im Zuge der Überarbeitung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken dieses Jahr.

Doch... wen meinen wir, wenn wir den «Staat» anrufen? Über viele Jahre hat die erzählte Katastrophe zur Aufrüstung von militärischen und nachrichtendienstlichen Kapazitäten geführt. Das Resultat davon ist die eingangs geschilderte Realität: staatliche Akteure sind heute viel aktiver im Cyberspace als noch vor zehn Jahren. Mehr Sicherheit wurde dadurch nicht generiert, im Gegenteil: konsequente Strafverfolgung und moderne, nachrichtendienstliche Fähigkeiten bedeuten die Nutzung von (möglichst unbekannten) Schwachstellen in der Informationsinfrastruktur zur Überwachung oder um Cyberoperationen durchzuführen, was heisst, dass solche Schwachstellen nicht gemeldet und geschlossen werden. Und doch hat «der Staat» gleichzeitig ein Interesse an der Nutzung von sichereren Technologien durch Wirtschaft und Gesellschaft – ein Zielkonflikt, der vor Augen führt, dass unterschiedliche Sicherheitsbegriffe auch innerhalb des Staates für Spannungen sorgen. Prägnanter: Aufrüstung im militärischen und nachrichtendienstlichen Bereich ist eine Quelle der Unsicherheit für Wirtschaft und Gesellschaft.

Spannungsfelder

Die Cybersicherheit in ihrer Breite ist ein typisches Querschnittsthema, das 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. Aufgrund unterschiedlicher Interessen entstehen mindestens drei Spannungsfelder, in denen jede Cybersicherheitspolitik positioniert werden muss. Verzerrte Gefahrenperzeption ist dabei nicht förderlich.

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. Dabei geht es in diesem Spannungsfeld um die Abhängigkeit von wirtschaftlichem Handeln und der daraus resultierenden Resilienz und Widerstandsfähigkeit des Gesamtsystems Gesellschaft. Also: mehr Staat beziehungsweise mehr Regulierung? Höchst punktuell vielleicht, aber man ist weit davon entfernt zu verstehen, wie im Sinne der nationalen Sicherheit gerecht und nicht markthemmend reguliert werden könnte. Stattdessen muss der Staat im Bereich der kritischen Infrastrukturen die Rolle eines Partners einnehmen und mit sogenannten öffentlich-privaten Partnerschaften für mehr Schutz und Resilienz sorgen. Dabei handelt es sich mehrheitlich um die freiwillige Zusammenarbeit der Wirtschaft mit dem Staat, vor allem im Bereich des Informationsaustauschs.

Im zweiten Spannungsfeld zwischen Staat und Bürger gilt es, die richtige Balance zwischen mehr Sicherheit und Freiheit im digitalen Raum zu finden. Der Staat erarbeitet sich im Rahmen seiner nachrichtendienstlichen Überwachungstätigkeiten, zum Beispiel bei der Terrorismusabwehr, der Spionageabwehr, aber auch bei der Vorbeugung von gewalttätigem politischem Extremismus, erhebliche Kompetenzen. Eine Vorgeschichte des Missbrauchs dieser Kompetenzen für ungerechtfertigte staatliche Eingriffe in die Bürgerrechte und gegenwärtige Beispiele aus anderen Weltregionen erzeugen eine Wahrnehmung des Staates als Gefahr für den Bürger. Mehr Staat? Lieber nicht. Denn je mehr Cyberkompetenzen ein Staat hat, desto höher ist das Risiko, dass sie eines Tages missbraucht werden, auch gegen die eigenen Bürger.

Im dritten Spannungsfeld zwischen Bürger und Wirtschaft gilt es die Rahmenbedingungen zu setzen für die Entwicklung eines erfolgreichen Sicherheitsökosystems. Wie kann der Markt, der 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?

In der Tat ist die Cybersicherheitspolitik also weniger auf das Verhindern und die Reaktion auf Cyberkatastrophen auszurichten, sondern als alltägliche Politik des Abwägens von Interessen und Werten, wie in anderen Bereichen auch. Je mehr Verständnis für die Normalität der Problematik, desto besser. Denn: Auch in Zukunft wird keine Cybersicherheitsstrategie der Welt je dazu führen, dass der digitale Raum gefahrenfrei wird. Die umfassende Gewährleistung von Sicherheit war noch nie möglich – und die Erwartung an staatliche Politik, einen solchen paradiesischen Zustand herzustellen, ist fehlgeleitet. Grundsätzlich sichere Gesellschaften müssen lernen, alltäglichen Risiken ohne Hysterie zu begegnen und auch in bezug auf Cybervorfälle nicht überzureagieren. Dabei ist es Aufgabe der Politik, die Tatsachen 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. ‹

Myriam Dunn Cavelty
ist Dozentin für Security Studies am gleichnamigen Center der ETH Zürich. Sie lebt mit ihrem Mann, dem Schriftsteller Gion Mathias Cavelty, ihrer Tochter und zwei Katzen in Zürich-Schwamendingen.