FIELD OF FOCUS 4
SELF-REGULATION AND REGULATION
INDIVIDUALS AND ORGANISATIONS

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

Journal of self-regulation and regulation

Volume 01 (2015)

Die materiellen Ursachen des Cyberkriegs
Cybersicherheitspolitik jenseits diskursiver Erklärungen

Myriam Dunn Cavelty

Abstract

Optimisten des Informationszeitalters sprachen Staaten jahrelang die Fähigkeit ab, ihre Macht im virtuellen Raum entfalten zu können. Jüngste Entwicklungen in der internationalen Politik zeigen jedoch, dass das Gegenteil zutrifft: Der Cyberspace wird mittlerweile von einer wachsenden/Mehrheit (Zahl) staatlicher Akteure als strategische Domäne angesehen, deren Weiterentwicklung und Steuerung nicht mehr nur nichtstaatlichen Akteuren überlassen werden kann. Staaten begegnen den von ihnen zunehmend ernst genommenen Cyberunsicherheiten, indem sie im Namen der nationalen Sicherheit mit wachsender Durchsetzungskraft Aspekte des virtuellen Raums ihrer Kontrolle unterwerfen. Vor dem Hintergrund dieser Zuspitzung analysiert dieser Beitrag spezifische Unsicherheitsfaktoren, die staatliches Handeln im Namen der nationalen Sicherheit im Cyberspace erklären und geht auf sich daraus ergebende Konsequenzen ein. Im Gegensatz zu der bisherigen Forschung in den Politikwissenschaften wird das Argument entwickelt, dass es nicht nur diskursive Prozesse in der Form von Sprechakten sind, die eine verstärkte Verknüpfung des Cyberspace mit der nationalen Sicherheit vorantreiben, sondern auch grundlegende technisch-materielle Faktoren und Praktiken, die sich der sozialwissenschaftlichen Forschung bisher weitgehend entziehen. Diese Dimension sollte vermehrt beachtet werden, wenn wir politische Cybersicherheitsprozesse und ihre Konsequenzen umfassender verstehen wollen.

Keywords

Cyberkrieg, Cybersicherheit, Kopenhagener Schule, Gouvernmentalität, „material turn“

DOI: 10.11588/josar.2015.0.23486

Die materiellen Ursachen des Cyberkriegs
Cybersicherheitspolitik jenseits diskursiver Erklärungen

Myriam Dunn Cavelty

1 Einleitung

Euphoriker des Informationszeitalters sprachen Staaten jahrelang die Fähigkeit ab, ihre Macht im virtuellen Raum entfalten zu können. Zu hierarchisch, langsam und unflexibel seien sie, um auf die entfesselte Dynamik des Cyberspace[1] und dessen Nutzung adäquat reagieren zu können (siehe z.B. Barlow 1996; Rosenau 1998). Jüngste Entwicklungen in der internationalen Politik zeigen jedoch, dass das Gegenteil zutrifft: Der Cyberspace wird als strategische Domäne angesehen, deren Aufbau und Steuerung nicht mehr nur nichtstaatlichen Akteuren überlassen werden kann. Staaten begegnen den von ihnen zunehmend ernst genommenen Cyberunsicherheiten, indem sie im Namen der nationalen Sicherheit mit wachsender Durchsetzungskraft Aspekte des virtuellen Raums ihrer Kontrolle unterwerfen (Schneier 2012, 2013; Meinrath et al. 2011). Da die Cyber-Domäne zu 100 Prozent menschengemacht ist und aufgrund von physischer Infrastruktur wie Kabeln und Servern auch gezwungenermaßen einer geographisch nationalstaatlichen Logik unterworfen ist, ist staatliche Machtausübung relativ einfach möglich – wenn auch zu einem bestimmten Preis (vgl. den Beitrag von Milton Mueller in diesem Band).

Auf Sicherheit zielende staatliche Interventionen, die diesen Raum nun einer nationalen Sicherheitslogik unterwerfen wollen, kollidieren häufig direkt mit rivalisierenden Vorstellungen, wie der Cyberspace ausgestaltet werden soll. Dies verursacht beträchtlichen Widerstand gegenüber nationalen Regulierungsversuchen, mit hohen Kosten für alle Beteiligten. Konkret führt die Bereitschaft von Staaten, Sicherheitsbedürfnisse über andere Bedürfnisse zu stellen, dazu, dass staatliche Kontrolle über Informationsflüsse und Bestrebungen, nationale Cyberräume zu bauen, sprunghaft zugenommen haben: Autoritäre Regime begrüßen dies, um ihre Macht weiter zu festigen (Deibert et. al. 2008, 2010; Deibert 2013). Auch in demokratischen Staaten gibt es mehr staatliche Überwachung und Zensur als je zuvor. Und je mehr sich der Diskurs um solche Kontrollversuche dreht, desto deutlicher geht es um physische Infrastrukturen, die den

1 In diesem Beitrag wird der Begriff Cyberspace anstelle des Begriffs Internet verwendet. Im populären Sprachgebrauch werden die zwei Begriffe oft als Synonyme gebraucht, in der sozialwissenschaftlichen Forschung aber wird das Internet als Teilaspekt des Cyberspace verstanden (vgl. Deibert et al. 2010). Der Cyberspace hat sowohl eine „virtuelle“ wie auch eine „physische“ Dimension.

Prinzipien der Territorialität und Souveränität unterworfen werden können und sollen (Dunn Cavelty 2015).

Im Zusammenhang mit der Zuspitzung, die das Thema der Cybersicherheit in den letzten Jahren erfahren hat, geht dieser Beitrag der folgenden Frage nach: Aufgrund von welchen Unsicherheitsfaktoren lässt sich der Anstieg von staatlicher Macht im Cyberspace erklären und welche Konsequenzen ergeben sich dadurch? Im Gegensatz zu der existierenden Forschung wird in diesem Beitrag das Argument entwickelt, dass es nicht nur diskursive Prozesse sind, die eine verstärkte Verknüpfung des Cyberspace mit der nationalen Sicherheit vorantreiben, sondern auch grundlegende technisch-materielle Faktoren und Praktiken, die sich der sozialwissenschaftlichen Forschung bisher weitgehend entziehen. Diese Dimension muss vermehrt beachtet werden, wenn wir politische Cybersicherheitsprozesse und ihre Konsequenzen (politischer, sozialer und wirtschaftlicher Natur) umfassender verstehen wollen.

Der Beitrag umfasst vier Teile. Im ersten wird die dominante Theorie in der Cyber-Sicherheitsforschung (*Securitization Theory*) kritisch im Hinblick auf ihre Erklärungskraft betrachtet und einige weiterführende theoretische Überlegungen angestellt, die zusätzliche Aspekte von Cybersicherheitspolitik in den Fokus rücken. Es wird eine Ergänzung der gängigen Analysen von eliteproduzierten, öffentlich zugänglichen Dokumenten durch den Einbezug von materiellen Unsicherheitsfaktoren und Sicherheitspraktiken propagiert. In einem zweiten Teil werden materielle Faktoren der Unsicherheit und ihr Einfluss auf die Cybersicherheitspolitik skizziert. In einem dritten Abschnitt werden drei Arten von auf diesen Faktoren beruhenden Konzeptionen des Cyberkriegs beschrieben. Dabei wird gezeigt, dass die Macht dieses Begriffs nicht nur in der Politik des „Worst Case" zu finden ist (vgl. Dunn Cavelty 2013a), sondern in seiner allumfassenden, andere Begrifflichkeit integrierenden/inkorporierenden Wirkung, die zu einem großen Teil auf materielle Unsicherheiten baut. Im letzten Teil werden die Wirkungen dieser Konzeptionen für die Cybersicherheit und allgemein die internationale Sicherheit aufgezeigt, die sich auch am besten auf materieller Ebene erschließen.

2 Theorie und Cybersicherheit

Einen genauen Zeitpunkt für den Anstieg von staatlicher Machtausübung im Cyberspace festzumachen, ist schwierig. Grund dafür ist unter anderem, dass es bisher keine zweckmäßigen Indikatoren gibt, die Dynamik staatlicher Macht in der Cyberdomäne über einen genügend langen Zeitraum zu messen.[2] Darüber hinaus zeichnen sich Cybersicherheitsdiskurse dadurch aus, dass es darin keinen einheitlichen, klar dominierenden Deutungsrahmen gibt. Stattdessen findet sich zu jeder Zeit eine Vielzahl von nebeneinander laufenden Diskursen, die sich auf unterschiedliche Aspekte der Prob-

2 Ein möglicher – aber nicht sehr valider – Indikator ist der Grad an „Internet freedom" (also Netzfreiheit), der z.B. von der Institution Freedom House erhoben wird (siehe: https://freedomhouse.org/issues/internet-freedom#.VVG9imP2P7Y). Das Problem dabei ist jedoch, dass staatliche Macht hier immer als Gegensatz zu Netzfreiheit verstanden wird.

lematik beziehen (Cyberkriminalität, Cyberterror, Cyberspionage, Cyberkrieg) und die unterschiedliche Lösungsansätze nach sich ziehen – die meistens einen Mix von staatlicher und nicht-staatlicher „Machtausübung“ beinhalten (Dunn Cavelty 2012). Wie im ersten Unterkapitel beschrieben wird, heißt das, dass eine der prominentesten Sicherheitstheorien, die Sekuritisierungstheorie der „Kopenhagener Schule” (Buzan et al. 1998), die sich mit den Wirkungen von Gefahrendarstellungen im politischen Prozess auseinandersetzt, nur sehr beschränkt Erklärungen für die Gründe für und Konsequenzen der Cybersicherheitspolitik liefert. Obwohl die Theorie in den letzten Jahren konstant weiterentwickelt und angepasst wurde, hat sie einige grundsätzliche Schwächen, die es verunmöglichen, dass sie die Dynamik der Cybersicherheitspolitik adäquat erklären kann. In einem zweiten Unterkapitel wird daher ein Vorschlag gemacht, welche Art von Theorie besser geeignet wäre.

2.1 Securitization Theory +

Die *Securitization Theory* sagt, dass die erfolgreiche *Securitization* (Versicherheitlichung) eines Themas den Einsatz aller verfügbaren Mittel rechtfertigt – insbesondere solche, die normale politische Spielregeln außer Kraft setzen. Um eine Versicherheitlichung zu erzielen, muss vorgängig eine mobilisierende diskursive Rechtfertigung für diesen außerordentlichen Zustand präsentiert werden, welche dann im politischen Prozess akzeptiert oder abgelehnt werden kann. Dies geschieht in der narrativen Darstellung der drohenden Gefahr (oder eines Risikos) und des dadurch bedrohten Referenzobjekts, in Form eines Sprechakts. Dabei erkennt die Theorie grundsätzlich nur eine Logik von Sicherheit an: eine Sicherheit, ohne die das Überleben (*survival*) (eines wertvollen Objekts, meist des Staats) gefährdet ist und die zu erreichen daher immer den Einsatz von außerordentlichen, den demokratischen Prozess sprengenden Maßnahmen rechtfertigt (vgl. Corry 2012).

Die Theorie (und diverse Abwandlungen davon) sind vereinzelt schon auf Cyberthemen angewandt worden (Bendrath 2003; Hansen et al. 2009; Lawson 2011). Dabei stand die Frage im Zentrum, ob der Themenkomplex Cybersicherheit insgesamt versicherheitlicht ist oder nicht. Die Literatur hat darauf keine einheitliche Antwort entwickelt: Je nach Schwerpunkt entweder auf die „multi-dimensional cyber disaster scenarios“ (Hansen et al. 2009: 1164) oder die tatsächlich umgesetzten Lösungen (Bendrath 2003) kommen die Autoren zu unterschiedlichen Schlüssen: erstere dazu, dass der Komplex versicherheitlicht ist; zweitere dazu, dass er es nicht ist. Allerdings sollte die Frage gestellt werden, ob die Feststellung, ob etwas versicherheitlicht ist oder nicht, überhaupt relevant ist, ohne dass die konkreten Konsequenzen der Versicherheitlichungsversuche aufgezeigt werden können. Die Theorie hat nämlich Mühe, heterogene Prozesse und über verschiedene Politikfelder fragmentierte Antworten auf Gefahren zu erklären, die nicht durchgehend der einen an „dem physischen Überleben (survival)“ geknüpften Logik von Sicherheit folgen (Neal 2009; Huysmans 2011).

Verschiedene Wissenschaftler haben über die Jahre versucht, diese Schwäche der Kopenhagener Schule durch Zusätze zu überwinden, die auch für Teilaspekte der Cybersicherheit relevant sind. Einige seien hier knapp skizziert. Jackson zum Beispiel (2006) hat das Konzept der „rhetorischen Versicherheitlichung" als eine Art Unterkategorie von gescheiterten Versicherheitlichungen eingeführt, bei der ein Sicherheitsproblem zwar als solches akzeptiert wird, dieser Prozess aber zu keiner außergewöhnlichen Maßnahme in der Politik führt. In der Tat finden wir die Cybersicherheit längst in nationalen Sicherheitsstrategien wieder – und doch ist es schwierig, den gesamten Themenkomplex als versicherheitlicht zu bezeichnen, insbesondere, wenn „außergewöhnliche“ Maßnahmen als ausschlaggebendes Kriterium angesehen werden, an denen es oftmals mangelt (Bendrath 2001; 2003). Andere Forschende haben festgestellt, dass der Prozess der Versicherheitlichung in einer bestimmten sozio-politischen Gemeinschaft nicht nur auf eine Arena und eine Art von Publikum beschränkt ist, sondern auch aus sich überlappenden Prozessen besteht (Balzacq 2005, 2008; Léonard et al. 2011). Damit ließen sich die Unterschiede in den Versicherheitlichungdynamiken für verschiedene Cybergefahrenkategorien bestimmen.

Andere wiederum schauen sich den zeitlichen Ablauf von Versicherheitlichungsprozessen an, um die Fixierung der Kopenhagener Schule auf einen bestimmten performativen Moment zu überwinden (Salter 2008: 575ff.). Versicherheitlichung ist dann vielmehr ein nie abgeschlossener Prozess, während dessen ständig neue Vorstöße gemacht werden und etablierte Versicherheitlichungslogiken aufrechterhalten werden müssen. Ähnliche Ansätze, die sich auf Versicherheitlichung als Prozess konzentrieren, entlang dessen Entscheidungsträger Herausforderungen kategorisieren können (von nicht-politisiert, zu politisiert, zu versicherheitlicht), lassen unterschiedliche und damit auch unterscheidbare „Grade“ von Versicherheitlichung zu (Haacke und Williams 2008; McDonald 2008). Mit einem solchen Ansatz ließen sich die unterschiedlichen (historischen) Phasen der Cybersicherheit und unterschiedliche Gefahrenkategorien und deren Wirkung besser verstehen und erklären, ohne den einen, ausschlaggebenden Moment der Versicherheitlichung identifizieren zu müssen.

2.2 Sicherheitspraktiken und die „little security nothings“

Mit den eben beschriebenen Zusätzen zur klassischen *Securitization Theory* können Dynamiken in der Cybersicherheitspolitik also teilweise erklärt werden. Der Theorie ist aber noch ein weiterer einschränkender Faktor zu Eigen. Wie fast alle diskurstheoretischen Ansätze schaut die Kopenhagener Schule fast ausschließlich auf „sichtbare” Sprechakte von politisch-öffentlichen Akteuren, die durch ein spezifisches Publikum akzeptiert werden können oder nicht (Huysmans 2011: 371). Securitization-Untersuchungen konzentrieren sich oft auf offizielle Aussagen von Staatsoberhäuptern, hochrangigen Beamten oder Leitern von internationalen Institutionen (Hansen 2006: 64). Dabei wird zumeist auf öffentlich zugängliche Dokumente (Reden, offizielle

Berichte, teilweise auch Bildmaterial etc.) zurückgegriffen, was aufgrund der einfachen Verfügbarkeit zu Vorteilen, aber auch durchaus zu einem „selection bias“ (einer Stichprobenverzerrung) führen kann. Solch ein Untersuchungsfokus vermag daher primär die konstitutive Wirkung von diskursiven Praktiken privilegierter Sprecher in der (Welt-)Politik aufzuzeigen. Was hingegen häufig kaum beachtet wird, ist wie diese diskursiven Praktiken durch zeitlich vorgelagerte sprachliche und nicht-sprachliche Praktiken von diesen und anderen Akteuren, die weniger leicht erkennbar oder attribuierbar sind, erleichtert oder vorbereitet werden.

Tatsächlich kann die Cybersicherheit als (sicherheits-)politisches Phänomen nur verstanden werden, wenn sie nicht nur mit Situationen von größter Dringlichkeit in Zusammenhang gebracht wird. Vielmehr geht es bei der Herstellung von Sicherheit im Cyberspace in erster Linie um alltägliche, „normale“ Routineprozesse und Verfahren, die entwickelt wurden, um Netzwerke, Computer, Programme und Daten vor Angriffen, Schäden oder unberechtigtem Zugriff zu schützen.[3] In Bezug auf die sicherheitsrelevanten Praktiken in bürokratischen Einheiten hat Jef Huysmans den Begriff der „little security nothings“ eingeführt (Huysmans 2011). So verstanden wird Cybersicherheit mitproduziert von jedem privaten Computerbenutzer, von IT-Support-Mitarbeitenden in den Serverräumen dieser Welt, von Programmierern, von Chief Information Officers (CIOs) oder Chief Executive Officers (CEOs), die Entscheide über Cybersicherheitsinvestitionen fällen, von IT-Spezialisten, die Regierungsnetzwerke sichern, von Sicherheitsberatern, von Cyberforensikern, von Regulierungsbehörden – und erst am Ende der cybersicherheitspolitischen Handlungskette von Politikern und anderen Regierungsbeamten, die Cybervorfälle interpretieren und auf sie mit verbalisierten Erwartungen und Befürchtungen und später auch Politiken reagieren.

Mit nicht klar eingrenzbaren politischen Phänomenen und solchen „little security nothings“ umzugehen weiß die Gouvernementalitätsforschung (vgl. Lemke et al. 2000). Gouvernementatlität ist ein Begriff, der auf Michel Foucault zurückgeht. Er versteht darunter

> „die Gesamtheit, gebildet aus den Institutionen, den Verfahren, Analysen und Reflexionen, den Berechnungen und den Taktiken, die es gestatten, diese recht spezifische und doch komplexe Form der Macht auszuüben, die als Hauptzielscheibe die Bevölkerung, als Hauptwissensform die politische Ökonomie und als wesentliches technisches Instrument die Sicherheitsdispositive hat“ (Foucault 2005: 171).

3 Cybersicherheit wird unter Experten nicht als Zustand, sondern als Prozess verstanden, der die Risiken, die aus dem Cyberraum jetzt und in Zukunft erwachsen, unter Berücksichtigung der IT-Schutzziele und unter Berücksichtigung der nötigen Funktionalität durch entsprechende Gegenmaßnahmen technischer, organisatorischer, rechtlicher und politischer Natur laufend auf ein gesellschaftlich akzeptiertes Maß zu reduzieren sucht. Die IT-Schutzziele im engen Sinne sind: Vertraulichkeit, Integrität, Verfügbarkeit, Authenzitität. Im erweiterten Sinne kommen hinzu: Zurechenbarkeit, Verbindlichkeit/Nicht-Abstreitbarkeit, Nicht-Anfechtbarkeit und in bestimmten Kontexten, wie z. B. im Internet, Anonymität. Die Basis für Cybersicherheit ist dabei in erster Linie die IT-Sicherheit und ihre Maßnahmen.

In den europäischen Sicherheitsstudien werden Gouvernementalitätsansätze seit einigen Jahren gewinnbringend auf komplexe und heterogene Probleme wie z.B. Terrorbekämpfung angewendet (siehe z.B. Aradau et al. 2007; Amoore et al. 2005). Ein solcher Ansatz erlaubt eine viel breitere Erfassung von Problemen, Konzepten, Techniken und Handeln in Bezug auf ein politisches Problem, als sie der Ansatz der Kopenhagener Schule ermöglicht. Forschende müssen sich nicht auf einen Teilaspekt und nicht nur auf eine Logik von Sicherheit beschränken. Insbesondere das Konzept des „Risikos" hat so verstärkt in der Sicherheitsforschung Fuß gefasst (Petersen 2012).

Methodisch-empirisch ergeben sich durch einen solchen Ansatz neue Herausforderungen. Nach wie vor können öffentlich zugängliche Dokumente studiert werden, dabei muss aber nicht auf Sprechakte geschaut werden. Häufig wird auch auf die historische Methode der sogenannten „Genealogie" à la Foucault zurückgegriffen, um das Entstehen und die Normalisierung von spezifischen Sicherheitsdispositiven zu erklären. Was jedoch als zusätzliches Element in den Blickpunkt rückt, sind Sicherheitspraktiken von Nicht-Eliten. Für die Forschung im Bereich der Cybersicherheit bedeutet dies, dass das Studium von öffentlich zugänglichen Dokumenten unbedingt und ganz im Sinne des „practice turns" (Schatzki et al. 2001) durch das Studium von Praktiken, soweit diese zugänglich sind,[4] ergänzt werden muss. Darüber hinaus erscheint es gewinnbringend, den Fokus auf die soziopolitischen Prozesse zu richten, die sich rund um Cybervorfälle (Schadsoftware, aber auch Hacktivismus- und Hackingkampagnen) abspielen.

2.3 Die technische Voraussetzung für Cyberunsicherheit

Dieser Beitrag kann dem Anspruch nach einer vertieften Analyse unter Einbezug von materiellen Faktoren und alltäglichen Praktiken nicht gerecht werden. Zumindest aber will er technisch-materielle Faktoren der Unsicherheit hervorheben und gleichwertig (oder ergänzend) neben Sprechakte stellen. Damit soll nicht behauptet werden, dass materielle Faktoren außerhalb und über politischen Entscheidungen und diskursiven Prozessen stehen. Dennoch bilden sie eine fundamentale Voraussetzung für die Art und Weise, wie die sicherheitspolitische Dimension der Cybersicherheit in Sprechakten etabliert werden kann. Neben einer Reihe von Trends im Bereich der Cybergefahren, die diese verstärkte Beachtung verursacht haben (vgl. z.B. Dunn Cavelty 2012b; 2015 – und siehe den folgenden Abschnitt), gibt es einige relativ konstant bleibende Faktoren der Unsicherheit, die mit den Technologien und deren Nutzung einhergehen, welche den virtuellen Raum ermöglichen und für diverse Akteure so attraktiv machen.

Fakt ist, dass digitale Technologien über die Jahre auf dem denkbar unsichersten Niveau im Cyberspace zusammengewachsen sind. Das hat teils historische Gründe, denn zu der Zeit, als das Internet für den wissenschaftlichen Datentransfer gebaut

4 Spätestens seit den Enthüllungen von Edward Snowden ist klar, dass die Geheimdienste und das Militär (oftmals in Kombination) zentrale Akteure im Bereich der Cybersicherheit sind. Ihre Praktiken bleiben jedoch bislang weitgehend unerforscht.

wurde, legten die Netzwerk-Designer mehr Gewicht auf die Robustheit und Ausfalltoleranz des Netzwerks als auf Sicherheitsaspekte. Aufgrund der wenigen (großen) Maschinen, die miteinander vernetzt waren, gab es dafür wenig Anlass. Die heutige Computernetzwerkumgebung ist deshalb so anfällig, weil sie aus der gleichen (unsicheren) Netzwerk-Technologie von damals besteht, diese aber mit viel offeneren (sprich ebenfalls unsicheren) Systemen kombiniert, die untereinander zudem stärker vernetzt sind (Libicki 2000; Warner 2012). Zudem hat die fortlaufende Globalisierung von Informationsnetzwerken zu einer drastischen Erhöhung der Komplexität geführt. Je komplexer ein IT-System aber ist, desto mehr Fehler enthält es; und desto schwieriger ist es, die IT-Sicherheit des Systems zu kontrollieren, zu gewährleisten oder zu verwalten. Das gleiche gilt für die verwendete Software.

Hinzu kommen ökonomische Gründe: Sehr schnelle Innovationszyklen bei IT-Produkten 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 angestrebte (oder erstrebenswerte) Sicherheitsstandard nie erreicht wird. Zudem haben Sicherheitsstandards oft einen negativen Effekt auf die Funktionalität und Benutzerfreundlichkeit (Andersson 2001). Auch ist der Softwaremarkt wegen des so genannten Netzwerkeffekts (der Nutzen an einem Produkt wächst, wenn dessen Nutzerzahl größer wird) geprägt von der Winner-takes-it-all-Logik und daraus hervorgehenden (Quasi-)Monopolen. In dem herrschenden hohen Kosten- und Zeitdruck bei der kommerziellen Software-Entwicklung wird daher meist nur auf die Funktionalität und eine schnelle Auslieferung geachtet. Qualitätskriterien, gerade in Bezug auf Sicherheit, spielen dabei eine untergeordnete oder gar keine Rolle. In den meisten Programmen und Betriebssystemen befinden sich daher unzählige (häufig nicht einmal bekannte) Sicherheitslücken, die zu ganz unterschiedlichen Zwecken missbraucht werden können – und werden.

Viele Attacken – die wirkungsvollsten bleiben häufig lange oder sogar für immer unerkannt – „beuten“ Sicherheitslücken aus, um auf das angegriffene System zugreifen zu können. Hat ein Angreifer Zugriff aus das Innenleben des Systems, kann er die sich darin befindenden Informationen zum Beispiel kopieren, korrumpieren, zerstören, abändern, stehlen, usw. (Waltz 1998). Abhängig vom Wert oder der Bedeutung der Informationen haben solche Aktionen unterschiedlich schwerwiegende Auswirkungen. Es ist daher unumstritten, dass Cyberangriffe Konsequenzen in der Form von z.B. Kosten haben. Das Beachtenswerte aus analytischer Sicht ist also nicht, dass den möglichen Gefahren des Cyberspace im politischen Prozess Beachtung geschenkt wird oder dass Überlegungen angestellt werden, ob der jeweilige Staat zusätzliche Anstrengungen zu ihrer Bekämpfung unternehmen soll. Hingegen ist bemerkens- und untersuchenswert, was oder wer zu welcher Zeit und durch wen die meiste Aufmerksamkeit (und welche Art von Ressourcen) erhält.

Dass Cybersicherheit als sicherheitspolitisches Problem angesehen wird, ist nicht selbsterklärend oder selbstverständlich, obwohl eine solche Deutung heute kaum

mehr hinterfragt wird. Es lässt sich beobachten, wie seit den 1980er Jahren im politischen Prozess verschiedene diskursive Verknüpfungen zwischen Cyberspace und anderen Themen und Objekten vorgenommen wurden, die zu dieser sicherheitspolitischen Deutung beigetragen haben – also z.B. neue Gefahrenkategorien wie Cyberterror geschaffen wurden. Eine große Rolle dabei spielte die „Form" des Cyberspace. Diese Prozesse sollen nicht Fokus dieses Beitrags sein, denn sie wurden anderswo bereits beschrieben (vgl. Dunn Cavelty 2010). Für die Ausführungen hier ist vor allem die Kopplung zwischen Computern (oder Informationsinfrastrukturen) und so genannten kritischen Infrastrukturen ausschlaggebend.

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. Als kritisch werden jene Infrastrukturen bezeichnet, die bei einem Ausfall zu gravierenden politischen oder wirtschaftlichen Schäden führen können (Dunn Cavelty et al. 2008; Collier et al. 2008).[5] Nach deren weitgehenden Privatisierung in den 1980er und 90er Jahren befinden sich viele dieser für die nationale Sicherheit wichtigen Objekte derzeit in privater Hand. Obwohl in vielen Sektoren Regulierungen bestehen, die auch die Sicherheit betreffen (häufig jedoch nicht direkt nationale Sicherheit, sondern eher die „Safety"),[6] folgen die Betreiber von kritischen Infrastrukturen grundsätzlich den Regeln des freien Markts und streben nach Gewinnmaximierung.

Neben klassischen Risiken wie Naturkatastrophen oder Feuer bilden Cybergefahren seit einigen Jahren eine neue Risikogruppe für kritische Infrastrukturen. Der Grund dafür ist, dass im Zuge von Automatisierungs- und Effizienzsteigerungsprozessen kritische Infrastrukturen häufig computerisiert wurden.[7] Ehemals isolierbare Geräte, wie industrielle Steuerungssysteme und Fabrikmonitore, die nun digital steuerbar und zugänglich gemacht werden, sind aber nie dafür entwickelt worden, mit dem Cyberspace verknüpft zu werden. Mit der steigenden Zahl von eingebetteten Systemen und mit deren wachsender Vernetzung untereinander (drahtlos wie auch kabelgebunden) er-

5 In diese Kategorie fallen gemeinhin die Energieversorgung, die Kommunikation, das Gesundheitswesen, der Verkehr oder die öffentliche Sicherheit. Die Bestimmung, was kritisch ist und was nicht, ist ein diskursiver Prozess, wohingegen die Verknüpfung von ehemals analogen Systemen mit digitalen Komponenten keiner ist.

6 „Safety" und „Security" werden auf Deutsch beide mit Sicherheit übersetzt und auch auf English sind die beiden Wörter sehr eng miteinander verbunden. In der technischen Community wird traditionellerweise das Wort „Safety" für Betriebssicherheit verwendet und das Wort „Security" für Angriffssicherheit (vgl. englische Übersetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie; Bundesministerium des Innern 2009: 3): „Sicherheitsstandard und die Ausfallsicherheit Kritischer Infrastrukturen" übersetzt als „safety standard and failure safety of critical infrastructure".

7 Es gibt sogar kritische Infrastrukturen, die sich mehr über Daten und Prozesse charakterisieren lassen, als über physische Komponenten (z.B. Finanzwesen) – eine solche Unterscheidung soll hier aber nicht gemacht werden.

höht sich damit objektiv gesehen deren Verwundbarkeit. Mit Hilfe von Suchmaschinen wie Shodan haben Forscher festgestellt, dass Millionen von Geräten, einschließlich solchen, die hochsensible Prozesse steuern, über das Internet zugänglich sind und dass 25–30 Prozent davon schlecht oder gar nicht gesichert werden und damit anfällig für Malware-Attacken sind (Jackson Higgins 2013).

Natürlich ist eine Schwachstelle in einem Computersystem, das kritische Prozesse steuert, noch nicht per se eine Bedrohung für die nationale Sicherheit. Das Wissen um diese Verwundbarkeiten und die Gewissheit, dass sie von böswilligen Akteuren ausgenutzt werden könnten, ist jedoch ein zentraler Bestandteil für die sicherheitspolitische Deutung der Cybersicherheit. Diskursive Prozesse setzen hier ein – die technische Unsicherheit ist die Basis dafür.

3 Drei Facetten des Cyberkriegs

Der Grund, warum Staaten heute mehr als früher bestrebt sind, Macht im Cyberspace auszuüben, ist in der Kombination von technisch-materiellen Faktoren und deren diskursiven Deutung/Verwertung im politischen Prozess zu finden. Seit jeher zeichnen sich Cybersicherheitsdiskurse nämlich dadurch aus, dass Cybervorfälle – die durch Schadsoftware oder DDoS-Attacken[8] hervorgerufen werden – herangezogen werden, um den Ernst der Lage für einen Akteur zu unterstreichen und um dann spezifische Ressourcen zu mobilisieren. Dabei ist es vor allem der Begriff des Cyberkriegs, der in vielen Facetten die Debatte dominiert. Bemerkenswert an diesem Begriff ist, dass damit weitaus nicht nur kriegsähnliche Formen der Cyberaggression bezeichnet werden; vielmehr sind es quasi alle Aggressionsformen, bei denen das Einwirken eines staatlichen Akteurs vermutet werden kann. Dadurch besetzt der Begriff „Cyberkrieg“ im Cybersicherheitsdiskurs eine hegemoniale Position, so dass alle daran Beteiligten und davon Betroffenen gezwungen sind, sich ihm ständig zu widmen, auch wenn sie ihn ablehnen. Der Begriff wird so laufend in seiner andere Logiken inkorporierenden Position bestärkt.

Die Effekte dieser Überdeterminierung liegen zum einen in der ständigen Mobilisierung von „Worst Case“-Szenarien als Beweis für die Dringlichkeit des Problems und in der Etablierung militärischer Zuständigkeit für Cyberfragen, was u.a. konkrete budgetäre Konsequenzen hat. Die Cyberverteidigung ist dann auch der eine Bereich, in dem die Ausgaben auch in Zeiten der allgemeinen militärischen Budgetkürzungen stetig steigen (Brito et al. 2011; Deibert et al. 2011). Zum anderen aber entsteht die Möglichkeit, die unterschiedlichsten Arten von Cybervorfällen als Cyberkrieg zu bezeichnen, eben durch die zuvor beschriebene technisch-materielle Logik. In den folgenden drei Unterabschnitten wird das Zusammenspiel zwischen technisch-materiellen Unsicherheitsformen und den diskursiven, politischen Elementen exemplarisch an drei „For-

8 DDoS-Attacke=Distributed Denial-of-service. Dabei wird ein Netzwerkdienst durch Überlastung nicht-verfügbar gemacht.

men“ des Cyberkriegs aufgezeigt. Das erste schaut sich den Cyberkrieg als Hacktivismus an. Das zweite die militärische Debatte zu Kriegsformen im Cyberspace. Das dritte analysiert „Advanced Persistent Threats“ (APTs), denen seit rund fünf Jahren besonders viel Aufmerksamkeit gewidmet wird.

3.1 Hacktivismus und seine sichtbaren Effekte

Der „Hacktivismus“ – ein Kofferwort aus „Hacking“ und „Aktivismus“ – hat sich spätestens seit der Kosovo-Intervention von 1999 als Form des politischen Protests etabliert: Heutzutage weist quasi jeder politische, wirtschaftliche und militärische Konflikt eine Cyberkomponente auf, die die eigentlichen Konflikthandlungen begleitet. Da der Hacktivismus neben unterschiedlichen Formen der Cyberkriminalität die weitaus häufigste Form von Cyberaggression ist, kommt ihm im allgemeinen Gefahrendiskurs eine sehr große Rolle zu. Durch die virtuelle Veränderung oder Zerstörung von Inhalten, wie z.B. dem Hacken von Webseiten oder dem Ausschalten eines Servers durch Datenüberflutung (DDoS-Attacke), kreiert der Hacktivismus „sichtbare“ Effekte (u. a. der Unterbrechung), die häufig, ganz im Sinne der Hacktivisten, medial ausgeschlachtet und aufgebauscht werden. Dabei steht er im Gegensatz zu anderen Cyberaggressionsformen, die keine sichtbaren Effekte kreieren, weil die Schadsoftware, die dahintersteckt, verborgen bleiben möchte.

Auch wenn eine systematische und empirisch saubere Auswertung von Hacktivismuskampagnen bisher fehlt, lässt sich doch festhalten, dass die Auswirkungen auf den eigentlichen Konflikt und dessen Verlauf fast ausschließlich marginal sind und der tatsächlich entstandene Schaden klein bis sehr klein bleibt. Der weitaus größere Effekt dieser digitalen Proteste entsteht im politischen Prozess, der Hacktivismus als Form des Cyberkriegs etabliert hat, auch wenn die Rolle von staatlichen Akteuren meistens unklar oder sogar fragwürdig bleibt.[9] Wie aber ist es möglich, dass dem Hacktivismus ein solcher Status in der sicherheitspolitischen Debatte zukommt?

Ein Fokus auf den Versicherheitlichungsprozess zeigt, wie die Vorfälle in Estland (2007) zum Beispiel[10] herangezogen werden, um die Realität des Cyberkriegs im Hier und Jetzt zu beweisen. Bemerkenswert dabei ist, dass die Details oder Annahmen hin-

9 Auch die Aktionen von WikiLeaks und der Hackerkollektive Anonymous oder LulzSec haben dem Hacktivismus unlängst sehr viel Aufmerksamkeit beschert – sie seien hier aber nur am Rande erwähnt. 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 greifen aufgrund der Medienwirksamkeit oft Ziele an, die als „kritische Infrastrukturen“ gelten und liefern so die Vorlage, um als nationales Sicherheitsproblem definiert zu werden (vgl. Dunn Cavelty et al. 2015).

10 Estland 2007 bezeichnet DDoS-Attacken auf Estland, die sich u.a. gegen das estnische Parlament, Banken, Ministerien und Rundfunksender richteten. Diese Attacken waren eine Begleiterscheinung eines Aufruhrs von russischen Esten, die gegen die Umstellung eines Denkmals protestierten. Der „cui bono“-Logik folgend, wurde die russische Regierung als Drahtzieher oder zumindest als Auftraggeber der Angriffe etabliert. Auch wenn eine Beteiligung nie bewiesen werden konnte, hält sich diese Attribution hartnäckig.

ter diesem Vorfall nicht mehr erläutert werden müssen: Es reicht, dass „Estland 2007“ gesagt wird, um ein Versicherheitlichungsargument zu machen. Das Wissen (und Nichtwissen) in Bezug auf diesen Vorfall hat sich im politischen Prozess zu einer spezifischen Wahrheit verdichtet, die Akteure wie Intentionen und Konsequenzen beinhaltet. Die Logik, die dabei zum Tragen kommt, ist die „cui-bono“-Logik. Die als „wem zum Vorteil“ zu übersetzende lateinische Frage drückt aus, dass der Verdacht am ehesten auf denjenigen fallen sollte, der durch eine (Straf-)Tat den größten Nutzen davonträgt. Im Falle von Estland 2007 weist die cui-bono Logik auf Russland hin, das mit Hilfe von nicht klar ihm zuordenbaren Aktivitäten im Cyberspace, die auf kritische Infrastrukturen abzielen, eine Machtdemonstration vornehmen will. Damit (staatlicher Akteur, der kritische Infrastrukturen angreift) lassen sich Aussagen von hochrangigen NATO-Generälen erklären, die sofort von einem potenziellen Bündnisfall sprachen.

Die „cui-bono“-Logik kann in diesem Diskurs nur eine so starke Stellung einnehmen, weil die technisch-materiellen Spielregeln des Cyberspace die gesicherte „Attribution“ (in etwa: Zuordnung) eines Angriffs äußerst schwierig, in gewissen Fällen sogar unmöglich machen. Das heißt: Clevere Gegner können sich vollkommen in der Anonymität des technischen Systems verbergen und gut gemachte Angriffe sind unmöglich einem exakten Ursprung zuzuordnen (Gaycken 2011: 80–90). 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 (Rid et al. 2015). So lassen sich auch die „Lösungsansätze“ erklären, die auf technischer Ebene die Attribution ermöglichen wollen, was gleichzeitig fast immer die Aufgabe von Anonymität im Cyberspace bedeuten würde.

3.2 Vom strategischen und operativen Cyberkrieg

Eine fachspezifischere Debatte zum Cyberkrieg spielt sich in strategisch ausgerichteten amerikanischen Fachjournalen ab. In öffentlichen Versicherheitlichungsprozessen sind solche Diskussionen nicht abgebildet, sie sind jedoch äußerst relevant, um gegenwärtige militärische Pläne und den Einsatz militärischer Mittel zu verstehen. In der Debatte wird zwischen dem strategischen und dem operationellen Cyberkrieg unterschieden. Der strategische Cyberkrieg bezeichnet einen Krieg, der ausschließlich mit Cybermitteln geführt wird oder bei dem andere Kampfhandlungen zumindest der Cyberdimension untergeordnet werden. Er wird wie folgt definiert: „hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence“ (Nye 2011: 21). In diesem Bereich befinden sich die klassischen Cyber-doom-Szenarien der 1990er Jahre, in denen vollkommen unsichtbare Feinde einem Land z.B. quasi per Knopfdruck den Strom abstellen und es so in die Knie zwingen.

Grundsätzlich hat sich bei den Experten die Meinung durchgesetzt, dass ein strategischer Cyberkrieg in der nahen Zukunft sehr unwahrscheinlich ist (Sommer et al. 2011; Rid 2011; Gartzke 2013). Dafür werden etwa die unsicheren Resultate eines virtuellen

Angriffs, die fehlende Motivation auf der Seite der möglichen Angreifer und deren gemeinsames Unvermögen, sich gegen einen Gegenschlag zu wappnen, genannt: alles Faktoren, die auf materielle Effekte hinweisen. Darüber hinaus werden unkontrollierbare Rückkopplungseffekte im stark vernetzten virtuellen Raum genannt, die beträchtliche Risiken auch für einen angreifenden Staat/Akteur bergen. Dieser Faktor ist umso wichtiger, als diejenigen Staaten, die das technologische Know-how für strategischen Cyberkrieg am ehesten besitzen oder entwickeln können, besonders abhängig von ihren eigenen Informationsinfrastrukturen und damit in einem potentiellen IT-Krieg sehr verletzlich sind. Aufgrund unkontrollierbarer Nebeneffekte wäre ein Cyberkrieg wohl auch mit einer langfristigen Destabilisierung des Vertrauens in den Cyberspace verbunden, was negative Folgen für die Weltwirtschaft und damit ebenfalls für alle Beteiligten nach sich ziehen könnte (Rathmell 2001).

Technisch-materielle Faktoren sind auch dafür verantwortlich, dass in strategischen Zirkeln der operative Cyberkrieg viel mehr Aufmerksamkeit findet. Der operative Cyberkrieg wird definiert als militärische Operationen begleitendes Phänomen, bei dem es zu staatlichen Cyberattacken auf militärische und zivile bzw. Dual-use-Infrastrukturen kommt (z.B. Telekommunikationseinrichtungen, die von zivilen Stellen unterhalten werden, jedoch für zivile und militärische Zwecke genutzt werden) und sich eine Beeinträchtigung auch auf die zivile Supply-Chain (bspw. zivile Auftragnehmer für Logistik) erstrecken könnte. Ein solches Szenario ist am sinnvollsten, wenn es um darum geht, militärische Reaktionen unmittelbar vor oder während einer konventionellen Kampfhandlung zu verlangsamen oder zu verunmöglichen (Libicki 2009: 82). Ganz spezifisch wird im US-Militär einem „Fait Accompli“-Szenario im Zusammenhang mit einer Konfrontation zwischen China und den USA wegen Taiwan am meisten Aufmerksamkeit geschenkt. In dieser spezifischen Cyberkriegsdebatte spielen Verwundbarkeiten in der Infrastruktur („Vulnerabilities“) die größte Rolle – die Einschätzung dessen ist der Hintergrund für konkrete Szenarien, die in die Planung für begleitende Kriegsführung im Cyberspace einfließen.

3.3 Advanced Persistent Threats

Die dritte Art des Cyberkriegs ist nicht zerstörerisch, sondern geheim und stetig. Gewisse Aspekte dieser dritten Art werden im öffentlichen Raum besprochen, andere hingegen vor allem in der technischen Fachdebatte. Die Cybersicherheitsdebatte hat sich seit 2010 beträchtlich zugespitzt, nicht zuletzt, weil sich beobachtbare Angriffsmuster substantiell verändert haben. In Gefahrenberichten von öffentlichen Stellen wie auch Privatunternehmen wird vor allem von der steigenden Professionalisierung auf dem kriminellen Markt berichtet, der längst nicht mehr von Einzeltätern, sondern von der organisierten Kriminalität beherrscht wird.

Diese Beobachtungen der Professionalisierung gehen einher mit einer Verschiebung der Aufmerksamkeit von Massenereignissen hin zu gezielten Angriffen („targeted

attacks“). Zum einen sind in den letzten Jahren vermehrt so genannte „Mega Hacks“ bekannt geworden, in denen große Datenmengen aus Firmen und regierungsnahen Einrichtungen gestohlen wurden. Auf der anderen Seite liegt der Schwerpunkt der Debatte jetzt auf sogenannten *Advanced Persistent Threats* (APTs) – Schadsoftware (und neu auch Hackingkampagnen), die relativ komplex sind und die nicht die massenhafte Ausbreitung zum Ziel haben (wie z.B. Spam oder normale Viren), sondern vor allem für das Eindringen in ein spezifisches Ziel (System) geschrieben wurden (Dunn Cavelty 2015).[11]

In der gesamten Malwareumgebung machen APTs nur einen kleinen Prozentsatz aus (Maillart et al. 2010), aber auf Grund ihrer Auswirkungen und ihrem Link zu strategischer Nutzung des Cyberspace erhalten sie große Aufmerksamkeit – wenn sie entdeckt werden. APTs ermöglichen schleichende und kontinuierliche Cyberoperationen, die bestimmte Informationen oder Funktionen von spezifischen Unternehmen oder Organisationen zum Ziel haben. Sie sind „advanced“ (fortgeschritten), da das Programmieren der Malware ein gewisses technisches Können voraussetzt. Sie sind „persistent“ (anhaltend), weil es eine ständige Überwachung der Malware von außen und oft eine konstante Extraktion von Daten gibt. Und sie werden in Übereinstimmung mit dem Vokabular der IT-Sicherheit als „threats“ (Bedrohung) bezeichnet, da sie von einem menschlichen Akteur orchestriert werden.

Für die meisten sind die technischen Determinanten von APTs der Beweis, dass Staaten die Anonymität des Cyberspace dazu ausnutzen, Cyberspionage durchzuführen. Erstens werden die Kosten für das Programmieren von APTs (und vor allem den gezielten Einsatz) als relativ hoch eingeschätzt, während es beim Hacktivismus sehr niedrige finanzielle und technische Eintrittsbarrieren gibt. Um bei Cyberoperationen einen kontrollierten Effekt zu erzielen, muss der „Angreifer“ Wissen über spezifische, bisher nicht bekannte und/oder nicht-gepatchte Schwachstellen besitzen und auch über die Fähigkeiten, diese mit Hilfe einer dafür geschriebenen Malware auszunutzen. Beides erfordert einen relativ hohen Organisationsgrad. Der Preis für strategisch wertvolle Schwachstellen liegt derzeit bei rund 200.000 bis 300.000 US-Dollar (Miller 2007; Böhme 2005). Diese lassen sich auf einem Graumarkt kaufen, auf dem Berichten zufolge auch Regierungen Kunden sind (Perlroth et al. 2013). Ein Bericht schätzt, dass z.B. die NSA im Jahr 2013 zwischen 100 und 625 Schwachstellen gekauft hat (Frei 2013:

11 Im als „Bundestag-Hack“ bekannt gewordenen Cyber-Vorfall (entdeckt im Mai 2015) wurde gemäß der zur Verfügung stehenden Informationen ein sogenannter Trojaner verwendet, der mit einem Klick auf einen Link in einer Email installiert wurde. Die Schadsoftware hat Daten aus dem IT-System des Bundestags kopiert und an Unbekannt versandt; typischerweise ist aber bisher noch nicht vollständig klar, welche Daten es waren und wie groß der Umfang war. Als Täter werden „östliche“ (bzw. russische) Geheimdienste vermutet. Über die technischen Details des Angriffs ist nicht viel bekannt (siehe aber Beuth 2015), aber da es sich um eine gezielte und wohl auch über eine Zeit andauernde Attacke handelt, gehört der Bundestag-Hack in die Kategorie APT. Die Aufklärung des Vorfalls dürfte lange dauern, mit ungewissem Ausgang (siehe etwa Bewarder et al. 2015; Gebauer et al. 2015).

15). Gemäß der Washington Post hat sie dafür über 25 Millionen Dollar bezahlt (Fung 2013). Darüber hinaus braucht es nicht nur gute Programmierkenntnisse, sondern auch „Labore“, in denen die Ziele simuliert werden können. Darüber hinaus scheint es plausibel, dass viele APTs physisch in die Zielsysteme eingeführt werden, also durch geschultes Personal vor Ort.

Bei dieser dritten Form des Cyberkriegs stehen also wieder Verwundbarkeiten in der Infrastruktur im Zentrum, aber auch die eigentliche Schadsoftware, die zu deren Ausnutzung eingesetzt wird. Aufgrund dieser Schadsoftware – und der sich um sie herum verdichteten Wahrheiten – wird wiederum gemäß der cui-bono-Logik auf die Akteure geschlossen, die dahinter stehen. Da hier große Verwundbarkeiten und staatliche Gegner mit ausreichenden Ressourcen und böswilliger Absicht verknüpft werden, kann die zunehmende Versicherheitlichung direkt mit dem Wissen um APTs einhergehen.

4 Der Cyberkrieg jenseits des Diskurses – Schlussbemerkungen

Von Hacktivismus bis APTs, aufsehenerregende Cybervorfälle sind heute an der Tagesordnung und finden zunehmend Beachtung auf höchster politischer Ebene. Wie im vorherigen Abschnitt exemplarisch aufgezeigt, werden dabei sehr unterschiedliche Formen von Cybervorfällen als Cyberkrieg bezeichnet. Die soziopolitischen Prozesse, die dabei zum Tragen kommen, sind nur teilweise gut erschlossen, gehen aber in fast allen Fällen weit über den „Sprechakt“, auf den sich der Sekuritisierungsansatz der Kopenhagener Schule gründet, hinaus. Die Gegenmaßnahmen, die diskutiert und umgesetzt werden, sind dabei äußerst vielschichtig und beinhalten technische, organisatorische, gesetzliche, außenpolitische und klassisch sicherheitspolitische Strategien und Instrumente. Analysen, die nur darauf schauen, wie über den Cyberkrieg „gesprochen“ wird, werden so nie die gesamte Breite der Cybersicherheitspolitik erfassen können.

Dies zeigt deutlich, dass die Forschung nicht nur darauf achten sollte, wer was zum Cyberkrieg sagt – sondern auch darauf, wer was tut und was die Konsequenzen dieser Taten sind. Einige dieser „Taten“ sind klar sichtbar und können mit traditionellen Ansätzen der internationalen Beziehungen erforscht werden. So können wir z.B. beobachten, dass trotz beträchtlicher Unterschiede zwischen herkömmlichen Sicherheitsproblemen und den neueren Herausforderungen der Cybersicherheit Staaten auf traditionelle Werkzeuge der Diplomatie setzen, um den Cyberspace international zu regulieren (Nye 2014). Während des Kalten Krieges entwickelte Instrumente werden verwendet, um politische Interaktion in und durch den Cyberspace zu stabilisieren und gleichzeitig das Eskalationspotential von Cyberkonflikten zu verringern. Der Schwerpunkt liegt auf dem Aufbau von Transparenz und Vertrauen bildenden Maßnahmen im Rahmen der OSZE sowie der Ausgestaltung von völkerrechtlichen Normen für kriegerische Auseinandersetzung im Cyberspace (Dunn Cavelty 2015). Wie und warum sich

welche Normen herausbilden und wer dabei welche Rolle spielt, bietet sich als Forschungsfrage regelrecht an; mittlerweile ist auch genügend Material vorhanden, um diese Normen-, vielleicht sogar eine internationale Regimebildung auch empirisch zu untersuchen.

Andere Praktiken sind weitaus schwieriger zu erforschen. Dazu gehören vorneweg geplante und bereits umgesetzte Konzepte der (operativen) Kriegsführung in und durch den Cyberspace. Während gewisse Grundideen in öffentlich zugänglichen Dokumenten abgebildet sind (z.B. in der im April 2015 veröffentlichten DoD Cyber Strategy), sind andere Sicherheitspraktiken nur über indirekte Zugänge erforschbar, auch wenn sie potentiell diejenigen sind, die einen direkten Einfluss auf die materielle Unsicherheit haben.

Es gibt viele Hinweise darauf, dass die rasante Entwicklung von militärischen und geheimdienstlichen Cyberkapazitäten gegenwärtig stärker wächst als das zivile Verständnis und die Möglichkeiten zu ihrer Kontrolle. Während Nachrichtendienste oft das Budget wie auch die nötigen technologischen Ressourcen besitzen, um auf Cyberbedrohungen reagieren zu können, löst ihre Rolle nicht erst seit Edward Snowdens Enthüllungen öffentliches Unbehagen aus. Solches Unbehagen ist nicht unbegründet: Im Namen der nationalen Sicherheit führen Praktiken dieser Akteure nämlich zu weniger Cybersicherheit – und so auch zu weniger Sicherheit für das Individuum. Das heimliche Einschleusen von Schadsoftware für Spionagezwecke in den Wirkungskreis von Nachrichtendiensten, aber auch bei Akteuren aus der Industrie hat bisher keinen sichtbar positiven Einfluss. Vielmehr scheint es so, als ob die nachrichtendienstliche Ausnutzung von Schwachstellen im Cyberbereich (z.B. durch APTs) jene Stabilität untergräbt, die durch die einsetzende internationale Normenbildung eigentlich erst noch erreicht werden soll. Absichtlich offen gehaltene Schwachstellen im globalen Cyberspace reduzieren die Sicherheit des gesamten Systems – für jedermann. Der strategisch nutzbare virtuelle Raum voller Schwachstellen und der sichere, robuste Cyberspace schließen sich gegenseitig aus. Darüber hinaus ist es äußerst besorgniserregend, wie leicht die gegenwärtig stattfindende Untergrabung der Freiheitsrechte (inkl. Privatsphäre) im Namen der Sicherheit zu rechtfertigen ist, ohne dass der Nutzen der Untergrabung nachgewiesen werden muss.

Die politikwissenschaftliche Cybersicherheitsforschung hat sich bisher vor allem mit Versicherheitlichungsprozessen durch Sprechakte befasst. Solche Analysen zeigen deutlich, welcher Stellenwert Cybergefahren im sicherheitspolitischen Prozess zukommt. Was diese Analysen aber nicht zeigen können, sind bereits existierende Praktiken, die Grund für, aber auch Konsequenz von solchen politischen Prozessen sind. Die hier entwickelte Perspektive soll es hingegen möglich machen, diese konkreten, bereits existierenden Auswirkungen auf die Sicherheit des gesamten Cyberspace in den Blick zu nehmen.

Literatur

Amoore, Louise / De Goede, Marieke (2005): Governance, Risk and Dataveillance in the War on Terror, in: Crime, Law and Social Change 43:2–3, 149–173.

Anderson, Ross (2001): Why Information Security is Hard – An Economic Perspective, in: IEEE Computer Society (Hrsg.): Proceedings of the 17th Annual Computer Security Applications Conference, IEEE Computer Society: Washington D.C., 358–365.

Aradau, Claudia / van Munster, Rens (2007): Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future, in: European Journal of International Relations 13:1, 89–115.

Balzacq, Thierry (2005): The Three Faces of Securitization: Political Agency, Audience and Context, in: European Journal of International Relations 11:2, 171–201.

Balzacq, Thierry (2008): The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies, in: Journal of Common Market Studies 46:1, 75–100.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace, https://homes.eff.org/~barlow/Declaration-Final.html (07.07.2015).

Bendrath, Ralf (2001): The Cyberwar Debate. Perception and Politics in US Critical Infrastructure Protection, in: Information & Security: An International Journal 7, 80–103.

Bendrath, Ralf (2003): The American Cyber-Angst and the Real World – Any Link?, in: Latham, Robert (Hrsg.): Bombs and Bandwidth: The Emerging Relationship between IT and Security, The New Press: New York, 49–73.

Beuth, Patrick (2015): Hackerangriff im Bundestag, in: Zeit Online, 12. Juni 2015, http://www.zeit.de/digital/datenschutz/2015-06/bundestag-hack-karlsruher-firma-aufklaerung (07.07.2015).

Bewarder, Manuel / Clauß, Ulrich (2015): Verfassungsschutz verfolgt Spur nach Russland, in: Die Welt, 11.06.2015, http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (07.07.2015).

Böhme, Rainer (2005): Vulnerability Markets – What is the economic value of a zero-day exploit? Paper given at the 2005 Chaos Communication Congress Berlin, Germany, https://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf (07.07.2015).

Brito, Jerry / Watkins, Tate (2011): Loving the Cyber Bomb? The Dangers of Threat Inflation, in: Cybersecurity Policy, Mercatus Center George Mason University, Working Paper No. 11–24.

Bundesministerium des Innern (2009): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf (03.08.2015).

Buzan, Barry / Wæver, Ole / de Wilde, Jaap (1998): Security: A New Framework for Analysis, Lynne Rienner: Boulder.

Collier, Stephen / Lakoff, Andrew (2008): The Vulnerability of Vital Systems: How Critical Infrastructure Became a Security Problem, in: Dunn Cavelty, Myriam / Kristensen, Kristian Søby (Hrsg.): The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitization, Routledge: London, 17–39.

Corry, Olaf (2012): 'Securitisation' and 'Riskification': Second-order Security and the Politics of Climate Change, in: Millennium – Journal of International Studies 40:2, 235–258.

Deibert, Robert / Rohozinski, Rafal (2010): Risking Security: Policies and Paradoxes of Cyberspace Security, in: International Political Sociology 4, 15–32.

Deibert, Ronald (2013): Black Code: Surveillance, Privacy and the Dark Side of the Internet, Random House: New York.

Deibert, Ronald / Palfrey, John G. / Rohozinski, Rafal / Zittrain, Jonathan (2008) (Hrsg.): Access Denied: The Practice and Policy of Global Internet Filtering, MIT Press. Cambridge.

Deibert, Ronald / Palfrey, John G. / Rohozinski, Rafal / Zittrain, Jonathan (2010) (Hrsg.): Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace, MIT Press: Cambridge.

Deibert, Ronald / Rohozinski, Rafal (2011): The New Cyber Military-Industrial Complex. The Globe and Mail, March 28, in: http://www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159/ (04.12.2012).

Dunn Cavelty, Myriam (2010): Cyber-security, in: Burgess, Peter (Hrsg.): The Routledge Companion to New Security Studies, Routledge: London, 154–162.

Dunn Cavelty, Myriam (2012): The Militarisation of Cyberspace. Why Less May Be Better, in: Czosseck, Christian / Ottis, Rain / Ziolkowski, Katharina (Hrsg.): Proceedings of the 4th International Conference on Cyber Conflict, Tallinn, 141–153.

Dunn Cavelty, Myriam (2013a): Der Cyber-Krieg der (so) nicht kommt – Erzählte Katastrophen als (Nicht)Wissenspraxis, in: Hempel, Leon / Bartels, Marie (Hrsg.): Aufbruch ins Unversicherbare – Zum Katastrophendiskurs der Gegenwart, Transcript Verlag: Bielefeld.

Dunn Cavelty, Myriam (2013b): From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, in: International Studies Review 15:1, 105–122.

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

Dunn Cavelty, Myriam / Jaeger, Mark Daniel (2015): (In)visible Ghosts in the Machine and the Powers that Bind: The Relational Securitization of Anonymous, in: International Political Sociology 9:2, 176–195.

Foucault, Michel (2005): Analytik der Macht, Suhrkamp: Frankfurt am Main.

Frei, Stefan (2013): The Known Unknowns. Empirical Analysis of Publicly Unknown Security Vulnerabilities, https://www.nsslabs.com/reports/known-unknowns-0 (07.07.2015).

Fund, Brian (2013): The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities, The Washington Post, 31 August 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/ (07.07.2015).

Gartzke, Eric (2013): The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth, in: International Security 38:2, 41–73.

Gaycken, Sandro (2011): Cyberwar: Das Internet als Kriegsschauplatz, München.

Gebauer, Matthias / Meiritz, Annett / Stöcker, Christian (2015): Cyberangriff auf Parlament: IT-Spezialisten können Bundestagstrojaner nicht stoppen, Spiegel Online, 21.05.2015, http://www.spiegel.de/netzwelt/netzpolitik/bundestag-experten-koennen-trojaner-nicht-stoppen-a-1035006.html 07.07.2015).

Haacke, Jürgen / Williams, Paul D. (2008): Regional Arrangements, Securitization, and Transnational Security Challenges: the African Union and the Association of Southeast Asian Nations Compared, in: Security Studies 17:4, 775–809.

Hansen, Lene / Nissenbaum, Helen (2009): Digital Disaster, Cyber Security, and the Copenhagen School, in: International Studies Quarterly 53, 1155–1175.

Huysmans, Jef (2011): What's in An Act? On Security Speech Acts and Little Security Nothings, in: Security Dialogue 42:4–5, 371–383.

Jackson Higgins, Kelly (2013): 'Project SHINE' Illuminates Sad State Of SCADA/ICS Security on the Net, Information Week, 16 October 2013. http://www.darkreading.com/vulnerabilities---threats/project-shine-illuminates-sad-state-of-scada-ics-security-on-the-net/d/d-id/1140691 (07.07.2015).

Jackson, Nicole J. (2006): International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework, in: Security Dialogue 37:3, 299–317.

Lawson, Sean (2011): Beyond Cyber-doom. Cyberattack Scenarios and the Evidence of History, in: Mercatus Center George Mason University Working Paper, No 11–01.

Lemke, Thomas / Krasmann, Susanne / Bröckling, Ulrich (2000): Gouvernementalität. Neoliberalismus und Selbsttechnologien. Eine Einleitung, in: Lemke, Thomas / Krasmann, Susanne / Bröckling, Ulrich (Hrsg.): Gouvernementalität der Gegenwart: Studien zur Ökonomisierung des Sozialen, Suhrkamp: Frankfurt am Main, 7–40.

Léonard, Sarah / Kaunert, Christian (2011): Reconceptualizing the Audience in Securitization Theory, in: Balzacq, Thierry (Hrsg.): Securitization Theory. How Security Problems Emerge and Dissolve, Routledge: London, 57–76.

Libicki, Martin (2000): The Future of Information Security, Institute for National Strategic Studies: Washington.

Libicki, Martin (2009): Cyberdeterrence and Cyberwar, RAND Corporation: Santa Monica.

Maillart, Thomas / Sornette, Didier (2010): Heavy-Tailed Distribution of Cyber-Risks, in: The European Physical Journal B, 75:3, 357–364.

McDonald, Matt (2008): Securitization and the Construction of Security, in: European Journal of International Relations 14:4, 563–587.
Meinrath, Sascha D. / Losey, Hames / Pickard, Victor (2011): Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide, in: The CommLaw Conspectus: Journal of Communications Law and Policy 19:2, http://scholarship.law.edu/commlaw/vol19/iss2/6/ (07.07.2015).
Miller, C. (2007): The legitimate vulnerability market: the secretive world of 0-day exploit sales. In 6th Workshop on the Economics of Information Security (WEIS 2007), http://www.econinfosec.org/archive/weis2007/papers/29.pdf (07.07.2015).
Neal, Andrew W. (2009): Securitization and Risk at the EU Border: The Origins of FRONTEX, in: Journal of Common Market Studies 47:2, 333–356.
Nye, Joseph (2011): Nuclear Lessons for Cyber Security? in: Strategic Studies Quarterly 5:4, 18–38.
Nye, Joseph (2014): The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance, http://dash.harvard.edu/bitstream/handle/1/12308565/NyeGlobalCommission.pdf?sequence=1 (07.07.2015).
Perlroth, Nicole / Sanger, David E. (2013): Nations Buying as Hackers Sell Flaws in Computer Code. New York Times, 13 July 203, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?partner=rss&emc=rss&smid=tw-nytimes&_r=1& (07.07.2015).
Peterson, Karen Lund (2012): Risk Analysis – a Field within Security Studies?, in: European Journal of International Relations 18:4, 693–717.
Rathmell, Andrew (2001): Controlling Computer Network Operations, in: Information & Security: An International Journal 7, 121–144.
Rid, Thomas (2011): Cyberwar Will Not Take Place, in: Journal of Strategic Studies 33:5, 727–758.
Rid, Thomas / Buchanan, Ben (2015): Attributing Cyber Attacks, in: Journal of Strategic Studies, 38:1–2, 4–37.
Rosenau, James (1998): Global Affairs in an Epochal Transformation, in: Henry, C. Ryan / Peartree, Edward C. (Hrsg.): Information Revolution and International Security, Center for Strategic and International Studies Press: Washington D.C., 33–57.
Salter, Mark B. (2008): Securitization and Desecuritization: A Dramaturgical Analysis of the Canadian Air Transport Security Authority, in: Journal of International Relations and Development 11:4, 321–349.
Schatzki, Theodore R. / Knorr, Cetina Karin / von Savigny, Eike (2001): The Practice Turn in Contemporary Theory, Routledge: London.
Schneier, Bruce (2012): When It Comes to Security, We're Back to Feudalism. Wired, http://www.wired.com/2012/11/feudal-security/ (07.07.2015).
Schneier, Bruce (2013): The Battle for Power on the Internet. The Atlantic, http://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/ (07.07.2015).
Sommer, Peter / Brown, Ian (2011): Reducing Systemic Cyber Security Risk. Report of the OECD's International Futures Project, IFP/WKP/FGS(2011)3: Paris.
Waltz, E. (1998): Information Warfare: Principles and Operations, Artech House: Boston.
Warner, M. (2012): Cybersecurity: A Pre-History, in: Intelligence & National Security 27:5, 781–799.

Autorin

Dr. Myriam Dunn Cavelty
Dozentin für Schweizerische und Internationale Sicherheitspolitik
Departement Geistes-, Sozial- und Staatswissenschaften
Eidgenössische Technische Hochschule Zürich
Haldeneggsteig 4
CH-8092 Zürich
dunn@sipo.gess.ethz.ch

DOI: 10.11588/josar.2015.0.23486

The **Journal of Self-Regulation and Regulation** is an open-access peer-reviewed journal serving as a potential outlet for edge-cutting interdisciplinary research on regulatory processes in individuals and organizations. It is published by the research council of Field of Focus 4 (FoF4) of Heidelberg University. The research council stimulates and coordinates interdisciplinary activities in research and teaching on self-regulation and regulation as part of the university's institutional strategy "Heidelberg: Realising the Potential of a Comprehensive University", which is funded by the Federal Government as part of the excellence initiative.

The *Journal of Self-Regulation and Regulation* publishes two volumes per year, regular volumes containing selected articles on different topics as well as special issues. In addition, the reader will be informed about the diverse activities of FoF4, uniting scientists of the faculty of behavioural and cultural studies, the faculty of social sciences and economics, as well as the faculty of law.

Imprint

Journal of Self-Regulation and Regulation Volume 01 (2015)

Research Council of Field of Focus 4, Heidelberg University
Forum Self-Regulation and Regulation
Hauptstr. 47–51
69117 Heidelberg, Germany

Fon: +49 (0)6221 / 54 – 7122
E-mail: fof4@psychologie.uni-heidelberg.de
Internet: https://www.uni-heidelberg.de/fof4

Publisher: Research Council of Field of Focus 4, Heidelberg University
Spokesperson: Sabina Pauen, Department of Psychology
Guest Editors: Wolf J. Schünemann, Department of Political Science
Sebastian Harnisch, Department of Political Science
Editorial Team: Melanie Bräunche, Sabine Falke

You can download the volumes of the *Journal of Self-Regulation and Regulation* free of charge at:
http://journals.ub.uni-heidelberg.de/index.php/josar/index