Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher und Jan W. Meine
Meine Verlag Magdeburg

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

IT-Sicherheit in der öffentlichen Wahrnehmung

Kristin Krüger

In der deutschen sicherheitspolitischen Debatte nimmt das Thema Sicherheit in der Informationstechnologie (IT) einen immer größeren Raum ein. Vor allem seit Stuxnet hat sich die öffentliche Wahrnehmung dieses Problemfeldes deutlich intensiviert. Auf welchen Ebenen das Thema IT-Sicherheit diskutiert wird und welche Meinungen die Öffentlichkeit zu diesem komplexen Thema hat, soll in diesem Aufsatz analysiert werden.

Zitationsvorschlag: Krüger, Kristin (2012). IT-Sicherheit in der öffentlichen Wahrnehmung. Magdeburger Journal zur Sicherheitsforschung, Band 1, 2012, S. 153–167.
http://www.wissens-werk.de/index.php/mjs/article/viewFile/111/108

Einleitung

> „Our reliance on cyberspace stands in stark contrast to the inadequacy of our cybersecurity – the security of the technologies that we use each day."[1]

In der deutschen sicherheitspolitischen Debatte nimmt das Thema Sicherheit in der Informationstechnologie (IT) einen immer größeren Raum ein. Vor allem seit *Stuxnet* hat sich die öffentliche Wahrnehmung dieses Problemfeldes deutlich intensiviert. Auf welchen Ebenen das Thema IT-Sicherheit diskutiert wird und welche Meinungen die Öffentlichkeit zu diesem komplexen Thema hat, soll in diesem Aufsatz analysiert werden.

Deutschland hat im Februar 2011, wie andere Staaten auch, eine nationale Cyberstrategie veröffentlicht.[2] Die besondere Bedeutung, die die IT-Infrastruktur im Gegensatz zu anderen Infrastrukturen inne hat, wird dabei häufig herausgestellt.[3] Die technologische Entwicklung hat es mit sich gebracht, dass die kritische IT-Infrastruktur mit den meisten anderen kritischen Infrastrukturen vernetzt ist. Sie unterscheiden sich von anderen dadurch, dass zwischen einem Angriff und dessen Folgen eine längere Zeit verstreichen kann. Jedoch ist dies nur ein Aspekt von IT-Sicherheit. Auch die Notwendigkeit einer globalen Zusammenarbeit wird in den jeweiligen Strategiepapieren herausgestellt.[4] Der Bedarf an internationalen Normen und Selbstverpflichtungen ist aufgrund der weltweiten Vernetzung, die der IT-Struktur immanent ist, eine Notwendigkeit, die zwar erkannt wurde und an deren Umsetzung gearbeitet wird, die aber bisher noch zu keinen Ergebnissen geführt hat. Auch die zu intensivierende Kooperation mit der Wirtschaft, vor allem aufgrund der kurzen Innovationszyklen im IT-Bereich, und die Sensibilisierung der Bevölkerung stehen auf der Agenda der Cyberstrategien.

Die Sensibilisierung der Öffentlichkeit soll auf zwei unterschiedlichen Ebenen erfolgen: Zum Einen soll der Bürger zu mehr Eigenverantwortung im persönlichen Umgang mit Computern angehalten werden, zum Anderen wird die Bevölkerung auf mögliche Gefährdungsrisiken aufmerksam gemacht, die der Gesellschaft drohen. Diese beiden Ansätze, ihre Vermittlung und die Rezeption in der Öffentlichkeit werden im vorliegenden Aufsatz thematisiert. Im Mittelpunkt steht dabei die Frage, welche Meinungen derzeit in der deutschen Öffentlichkeit zum Thema „Cybersecurity"5 vorherrschen und ob sich daraus tiefer liegende Einstellungen ableiten lassen. Dies wird für die beiden angeführten Ebenen untersucht. Zuvor wird die angewendete Theorie zur Meinungsbildung in der Öffentlichkeit dargelegt. Im Hauptteil wird die Fragestellung anhand des Beispiels der Vorratsdatenspeicherung erforscht. Des Weiteren wird das Verhältnis des mündigen Internetbürgers zum Staat untersucht.

1 Department of Defense (2011). Strategy for Operating in Cyberspace. http://www.defense.gov/news/d20110714cyber.pdf (17.07.2011). S. 1.

2 Bundesministerium des Innern (2011). Cyber-Sicherheitsstrategie für Deutschland. http://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Sicherheit/css_download.pdf?__blob=publicationFile (17.07.2011).

3 Bundesministerium des Innern, 2011; Department of Defense, 2011.

4 Ebd.

5 Der Autorin ist bewusst, dass der Begriff „Cyber" in allen Kombinationen inflationär gebraucht wird und die Bedeutung desselben alles andere als eindeutig ist. In Ermangelung eines passenderen (deutschen) Begriffes wird dieser jedoch auch in diesem Aufsatz verwendet, um das Spektrum der Bedeutungen, die in diesem Begriff mitschwingen, abzudecken. Die englischen und die deutschen Fachbegriffe aus dem Bereich der IT-Sicherheit werden in diesem Aufsatz gleichberechtigt verwendet.

Eine überblicksartige Darstellung der verschiedenen Ebenen von IT-Sicherheit wird im Folgenden vorgenommen, um im Anschluss die Frage nach der Darstellung des Themenkomplexes in den Medien zu analysieren. Das Schlusskapitel gibt einen kurzen Gesamtüberblick über die Ergebnisse und fasst die deutsche öffentliche Meinung zum Thema IT-Sicherheit zusammen.

1. Öffentliche Meinung – „One man, one vote"?

Der Begriff der „öffentlichen Meinung" hat sich im Laufe der Zeit stark gewandelt und bezieht sich heute hauptsächlich auf das Feld der Politik. Auch die Erforschung der öffentlichen Meinung hat sich verändert. Es gibt verschiedene Theorien darüber, wie sich eine öffentliche Meinung herausbildet. In den 1950er und 60er Jahren herrschte noch das Elitenkonzept vor, vertreten bspw. durch Wilhelm Hennis und Herbert Blumer. Einen ähnlichen Ansatz vertraten Lippmann und Almond, deren Theorien unter dem Begriff „Almond-Lippmann-Komplex" bekannt wurden.

> „According to Lippmann, the common man is too fully engaged in the requirements of earning a living and otherwise attending to his most immediate needs to have the time or inclination to satisfy the heroic, but clearly unrealistic, assumptions about the informed and engaged citizen celebrated in classical democratic theory. The chasm between theory and reality is especially wide on foreign affairs, which are typically far removed from the direct experiences of the mass public."[6]

Die Annahme, dass die Bevölkerung wenig an Außen- und insbesondere an Sicherheitspolitik interessiert sei, besteht bis heute fort. Gibt es jedoch konkrete Anlässe, wie bspw. die Bedrohung durch einen atomaren Erstschlag während des Kalten Krieges, rückt die Außen- und Sicherheitspolitik verstärkt in den Fokus der medialen Wahrnehmung und es erweist sich, dass die Öffentlichkeit durchaus eine fundierte Meinung dazu hat. Nach Einschätzung der Autorin könnten die Themenkomplexe rund um die Cybersicherheit zu einem ähnlichen Phänomen führen.

Ole Holsti, von dem obiges Zitat stammt, stimmte noch 1992 den Annahmen des Almond-Lippmann-Komplexes grundsätzlich zu:

> „Not only do polls repeatedly reveal that the mass public has a very thin veneer of factual knowledge about politics, economics and geography; they also reveal that it is poorly informed about the specifics of conflicts, treaties, negotiations with other nations, characteristics of weapon systems, foreign leaders and the like."[7]

Holsti verwies noch in demselben Artikel darauf, dass die Gegenargumentation von Page und Shapiro, erstmals veröffentlicht 1988 in einem Artikel im ‚Journal of Conflict Resolution', nicht haltbar ist, weil sie nicht auf Panelstudien aufbaut und die Frage nach der Volatilität nicht beantwortet. Doch diese Meinung wurde noch im gleichen Jahr durch das Erscheinen des Gesamtwerkes von Page und Shapiro erschüttert. Die Autoren widerlegen hier auf Grundlage einer breiten empirischen Basis (inkl. Panelstudien) die Annahme, dass die politischen Einstellungen der Bevölkerung

6 Holsti, O. R. (1992). Public Opinion and Foreign Policy: Challenges to the Almond-Lippmann Consensus, Mershon Series: Research Programs and Debates, S. 440f.

7 Ebd. S. 447.

nicht rational sind. Das bedeutet nicht, dass die Einstellungen eines Individuums keinen Schwankungen unterworfen sind, aber gesamtgesellschaftlich betrachtet beruht die öffentliche Meinung auf ihr zugrunde liegenden, stabilen Einstellungen. Page und Shapiro werten Umfragedaten der amerikanischen Bevölkerung von 1930 bis Anfang der1990er Jahre aus und kommen dabei zu dem Schluss, dass die Daten gegen die Aussagen des Almond-Lippmann-Komplexes sprechen. Da die Theorie von Page und Shapiro die Ausgangslage für die weitere Argumentation darstellt, werden die Hauptargumente in einem ausführlichen Zitat wiedergegeben:

> „The main argument is that the collective policy preferences of the American public are predominantly rational, in the sense that they are real–not meaningless, random "nonattitudes"; that they are generally stable, seldom changing by large amounts and rarely fluctuating back and forth; that they form coherent and mutually consistent (not self-contradictory) patterns, involving meaningful distinctions; that these patterns make sense in terms of underlying values and available information; that, when collective policy preferences change, they almost always do so in understandable and, indeed, predictable ways, reacting in consistent fashion to international events and social economic changes as reported by the mass media; and, finally, that opinion changes generally constitute sensible adjustments to the new conditions and new information that are communicated to the public."[8]

Mehrere Aspekte dieses Zitats sind für die weitere Analyse von Bedeutung: Zum Einen ist die öffentliche Meinung stabil, passt sich aber gleichzeitig auch neuen Gegebenheiten an. Dies passiert auf der Grundlage der verfügbaren Informationen, die hauptsächlich durch Massenmedien verbreitet werden. Zum Anderen reagiert die Öffentlichkeit mit rationalen Korrekturen ihrer zugrunde liegenden Einstellungen auf neue Situationen.

Bevor die Autorin diese Aspekte in Bezug auf IT-Sicherheit untersucht, soll kurz das Verhältnis von Meinung, Einstellung und Werten erläutert werden. Hierbei handelt es sich um ein sozialpsychologisches Konstrukt, dass von der Soziologie adaptiert wurde und vor allem in der Wahl- und Marktforschung angewendet wird. Es beruht auf dem Dreikomponentenmodell von Rosenberg und Hovland aus dem Jahr 1960.[9]

Man geht in der Soziologie von einem dreistufigen Modell aus, bei dem Meinungen Antworten auf konkrete Fragestellungen sind. Sie sind hoch volatil und meist kurzfristig, beruhen jedoch auf zugrunde liegenden Einstellungen. Diese Einstellungen steuern das Verhalten des Individuums und bestehen aus drei Komponenten (angelehnt an Rosenberg/Hovland). Die kognitive Komponente besteht hauptsächlich aus Wissen und Informationen über das Einstellungsobjekt. Dazu kommen die affektive Komponente, die sich aus subjektiven Gefühlen zusammensetzt und die Verhaltenskomponente, bestehend aus einer bestimmten Verhaltenstendenz oder -absicht. Letztere Komponente umfasst auch häufig die Rahmenbedingungen in einer konkreten Situation. Einstellungen beziehen sich demzufolge auf Sachverhalte, über die man

8 Page, B. I. & Shapiro, R.Y. (1992). The rational public: fifty years of trends in Americans' policy preferences, S. xi.

9 Vgl. Herle, M. & König, D. (2002): Einstellungen. http://dk.akis.at/einstellungen.html (13.08.2011).

bereits nachgedacht hat und sind nicht so volatil wie Meinungen, auch wenn sie von affektiven Komponenten beeinflusst werden. Den Einstellungen eines Individuums liegen wiederum Wertorientierungen zu Grunde. Diese lassen sich bei einem Individuum kaum ändern und bestimmen in ihrer gesellschaftlichen Gesamtheit meist einen Kulturkreis. Zu einem Wertewandel kommt es meist nur durch einen Generationenwechsel.

Bei Umfragen kann man zwischen Meinungen, Einstellungen und Werteorientierungen nicht differenzieren. Meist geht man davon aus, dass Meinungen abgefragt werden. Bei Panelumfragen werden die gleichen Personen über einen längeren Zeitraum immer wieder befragt. Aber auch hier zeigt sich, dass man davon nicht zwangsläufig auf Einstellungen schließen kann. Page und Shapiro führen an, dass bei den National Election Studies von 1956, 1958 und 1960 zu der Frage, ob die Versorgung mit elektrischem Strom entweder von Privatfirmen oder dem Staat erfolgen sollte, nur 24 Prozent der Befragten konsequent bei einer Meinung blieben.[10]

Es kann demzufolge nicht zweifelsfrei festgestellt werden, bei welchen Ergebnissen einer Umfrage es sich um Meinungen und bei welchen es sich um Einstellungen handelt. Somit ist es durchaus denkbar, dass die befragte Menge bei der nächsten Befragung ihre Meinung ins Gegenteil geändert hat. Damit bleibt die Frage nach den Gründen für die Volatilität offen. Der entscheidende Aspekt ist jedoch laut Page und Shapiro, dass sich die Meinungen gesamtgesellschaftlich gesehen kaum ändern.[11] In der Masse, die ja auch die öffentliche Meinung bildet, bleibt der Anteil der Menschen, die eine jeweilige Meinung vertreten, gleich. Somit lässt sich berechtigterweise davon ausgehen, dass es sich hierbei um Einstellungen innerhalb eines Kulturkreises handelt.

Die Autorin geht davon aus, dass die Ergebnisse von Page und Shapiro auf die deutsche Bevölkerung übertragbar sind. Da der Begriff der öffentlichen Meinung in der deutschen Wissenschaftsdiskussion sehr umstritten ist,[12] orientiert sich die Autorin an der amerikanischen Begriffsbestimmung und damit an der Definition von Frank Brettschneider:

> „Im folgenden wird unter öffentlicher Meinung die Verteilung der in Umfragen gemessenen individuellen Einstellungen zu politischen Sachfragen in einem repräsentativen Querschnitt der Bevölkerung verstanden."[13]

Für die Umfragen in Bezug auf die IT-Sicherheit sind diese theoretischen Erkenntnisse von entscheidender Bedeutung. Vor allem die theoretischen Grundlagen von Page und Shapiro werden in den folgenden Kapiteln wieder aufgegriffen.

2. Gibt es überhaupt eine öffentliche Meinung zur IT-Sicherheit?

> „Auf Gefahren im Netzwerk reagieren viele Nutzer zwiespältig. Einerseits verdrängen sie solche Gefahren um des Genusses willen, so dass nicht jedes Mal die Frage nach der Funktionsfähigkeit und vor allem der persönlichen Sicherheit aufkommt, wenn sie ihre Rechner einschalten. […] Andererseits bleibt bei vielen Nutzern ein Gefühl

10 Page & Shapiro, 1992, S. 6.

11 Page & Shapiro, 1992, S. 20.

12 Vgl. Brettschneider, F. (1995). Öffentliche Meinung und Politik: eine empirische Studie zur Responsivität des Deutschen Bundestages zwischen 1949 und 1990, S. 23 f.

13 Ebd. S. 24.

> der Unsicherheit über die Sicherheit im Internet: Vieles bleibt unwägbar, undurchsichtig […]."[14]

Die deutsche Bevölkerung hat zweifellos eine Meinung zum Thema IT-Sicherheit, nur wird diese bisher kaum gemessen. Die derzeitigen Umfragen beziehen sich entweder auf ein singuläres Ereignis, wie bspw. die Vorratsdatenspeicherung, oder aber auf allgemeine Fragen zum Internet, z. B. Nutzungsdauer etc. Außerdem handelt es sich bei den Umfragen, die in diesem Zusammenhang durchgeführt wurden häufig um kurzfristige Meinungsbilder. Langfristig angelegte Studien, die sich mit dem Thema IT-Sicherheit in Deutschland nicht nur am Rande auseinandersetzen, wurden nach Wissen der Autorin bisher nicht veröffentlicht. Die Einstellungen können insofern nur indirekt gemessen werden. Als Indikatoren wird die Autorin im Folgenden ein konkretes Ereignis und die mediale Wahrnehmung von Themen der IT-Sicherheit analysieren, um dann Schlussfolgerungen über die öffentliche Meinung zum Thema zu ziehen. Bei dem untersuchten Ereignis handelt es sich um die lange diskutierte Vorratsdatenspeicherung. Sie markiert einen Einschnitt in der öffentlichen Wahrnehmung. Die Debatte um die Vorratsdatenspeicherung ist die erste öffentliche Diskussion, die auch außerhalb der Fachmedien das Thema „Internet" und „Sicherheit in puncto Datenschutz im Internet" aufgreift.

2.1 Die Vorratsdatenspeicherung

Die Einführung der Vorratsdatenspeicherung zum 01. Januar 2008 hat zur größten Verfassungsbeschwerde in der Bundesrepublik Deutschland geführt. Knapp 35.000 Bürger haben einen Rechtsanwalt damit beauftragt, Verfassungsbeschwerde zu erheben. Es gab eine umfangreiche öffentliche Diskussion in allen Medien, an der sich auch viele Politiker beteiligt haben. Die deutsche Bevölkerung scheint hinsichtlich der Vorratsdatenspeicherung gespaltener Meinung zu sein. Laut einer Forsa-Umfrage im Auftrag des Magazins „Stern" im Juni 2007 halten 54 Prozent der Befragten (n=1000) die sechsmonatige Speicherung aller Verbindungsdaten für einen unzulässigen Eingriff in die Freiheitsrechte der Bürger.[15] Auch nach der Einführung der Vorratsdatenspeicherung zeigt sich ein ähnliches Bild: 46 Prozent von 1002 Befragten im Auftrag des Arbeitskreises Vorratsdatenspeicherung halten die Vorratsdatenspeicherung nicht für eine notwendige Maßnahme zur Verbrechensbekämpfung, sondern für einen unzulässigen Eingriff in die eigenen Freiheitsrechte.[16] Im Gegensatz dazu hielten 48 Prozent die Maßnahme für nützlich.[17]

In derselben Umfrage wurde nach der Kontaktaufnahme zu sensiblen Einrichtungen, wie Eheberatungsstelle, Psychotherapeut oder Drogenberatung per Telefon oder E-Mail gefragt. Insgesamt 46 Prozent der Befragten würden den Kontakt aufnehmen, im Gegensatz zu 52 Prozent, die den Kontakt aufgrund der Speicherung der Verbindungsdaten eher unterlassen würden.

14 Fischer, W. (2007). www.InfrastrukturInternet-Cyberterror.Netzwerk. Analyse und Simulation strategischer Angriffe auf die kritische Infrastruktur Internet, S. 14.

15 Forsa & Stern (2007). Sicherheitsmaßnahmen - Verletzung der Freiheitsrechte der Bürger. http://de.statista.com/statistik/daten/studie/151237/umfrage/sicherheitsmassnahmen-die-als-eingriff-in-die-freiheitsrechte-empfunden-werden/ (9.10.2011).

16 Forsa & Arbeitskreis Vorratsdatenspeicherung (2008). Meinungen der Bundesbürger zur Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf (09.10.2011), S. 5.

17 Ebd.

Eine repräsentative Umfrage des Instituts für Demoskopie in Allensbach stellte im Jahr 2009 fest, dass „mehr als jeder Zweite aus der Bevölkerung (52 Prozent) betont, dass er in letzter Zeit vorsichtiger geworden ist, wenn irgendwo persönliche Daten abverlangt werden."[18] Dies kann man so interpretieren, dass die öffentliche Diskussion in der Bevölkerung zu einem bewussteren Umgang mit persönlichen Daten geführt hat. Es ist möglich, dass die Debatte um die Vorratsdatenspeicherung einen Anteil daran hatte. Denn wie die Umfrage zeigt, misstrauen die Befragten den Unternehmen zwar deutlich häufiger (82 Prozent), aber immerhin 72 Prozent misstrauen auch dem Staat beim Umgang mit ihren gespeicherten Daten.[19] Nur 16 Prozent der Befragten vertrauen dem Staat diesbezüglich.

Bei einer repräsentativen Umfrage des Instituts für Demoskopie in Allensbach im Auftrag von T-Systems[20] steht bei der Frage nach Risiken, die aus Sicht der Befragten in Deutschland zukünftig zunehmen werden, der Missbrauch von persönlichen Daten an erster Stelle. Insgesamt 70 Prozent sind der Meinung, dass dieser steigen werde. An zweiter Stelle (70 Prozent, Mehrfachnennungen möglich) steht die Meinung, dass sich auch der Datenbetrug im Internet erhöhen wird. Der Ansicht, dass Computerviren häufiger auftreten werden, sind immerhin noch 60 Prozent der 1751 Befragten. Hingegen gehen bei der Frage, ob der Staat seine Bürger zu sehr überwacht, nur 42 Prozent von einem steigenden Risiko aus und 38 Prozent denken, dass sich diesbezüglich nicht viel ändern wird. Die Gefahren, die mit dem Komplex IT-Sicherheit einhergehen, werden insgesamt überwiegend als zunehmend bewertet.

Die Vorratsdatenspeicherung ist wahrscheinlich das öffentlich meistdiskutierte Thema im sicherheitspolitischen Bereich der IT-Sicherheit. Trotzdem entbehrt die Datengrundlage einer breiten, wissenschaftlich fundierten Basis. Aus den punktuellen Meinungen scheint sich jedoch ein zwiespältiges Bild abzuzeichnen. Die Maßnahmen, die der Staat im Bereich der IT-Sicherheit unternimmt, scheinen stark zu polarisieren. Das ohnehin nur mittelmäßig ausgeprägte Vertrauen in die Bundesregierung[21] wird weiterhin unterminiert, wenn gesetzlichen Maßnahmen vom Bundesverfassungsgericht in Karlsruhe gekippt werden. Dies war nicht nur bei der Vorratsdatenspeicherung der Fall, sondern auch bspw. beim ersten Entwurf zum Bundestrojaner.

Die öffentliche Meinung zur Vorratsdatenspeicherung ist den Umfragen zufolge relativ ausgeglichen zwischen ablehnend und zustimmend verteilt. Die einzelnen Stichproben lassen jedoch keine Aussage über die Entwicklung im Zeitverlauf zu.

2.2 Der mündige Internetbürger und der Staat

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt eine eigene Webseite, auf der der interessierte Bürger sich umfassend über aktuelle Gefahren im Internet informieren kann und Anlei-

18 Institut für Demoskopie Allensbach (2009). Zu wenig Datenschutz? Die meisten sind mit persönlichen Daten vorsichtiger geworden. In Allensbacher Berichte, Nr. 6, S. 3.

19 Ebd. S. 2.

20 Deutsche Telekom/T-Systems (2011). Sicherheitsreport 2011. Eine repräsentative Studie zum Thema Sicherheit in Deutschland im Auftrag von T-Systems. http://www.download-telekom.de/dt/StaticPage/10/84/08/T-Systems_Sicherheitsreport_2011.pdf_1084082.pdf (30.11.2011), S. 16.

21 Simonson, J. (2003). Entwicklung und Struktur des Institutionenvertrauens. Empirische Analysen auf Basis der ALLBUS-Daten. http://www.sozialforschung.uni-bremen.de/English/Downloads/P2003/vertrauen.pdf (09.10.2011), S. 3.

tungen zum sicheren Umgang mit dem Internet und für Schutzvorkehrungen des eigenen Endgeräts bekommt.[22] Gleichzeitig spielt das Thema IT-Sicherheit in der öffentlichen Wahrnehmung nur eine untergeordnete Rolle. In den Medien wird es nur dann besprochen, wenn sich ein besonders spektakulärer Wurm, Trojaner oder ähnliches verbreitet, der zu direkten Konsequenzen auf den Endgeräten der Nutzer führt. Handelt es sich um eine Schadsoftware, die versteckt im Hintergrund agiert, aber zu keinen Einschränkungen beim Endnutzer führt, erfährt diese deutlich weniger mediale Aufmerksamkeit wie bspw. bei *Zeus*.

Des Weiteren hat eine Umfrage des BSI ergeben, dass die Bürger zwar um die Gefahren des Internets wissen und auch wissen, dass sie selbst für ihren Schutz verantwortlich sind (86 Prozent der Befragten), aber trotzdem „[…] ist über die Hälfte der Befragten (53 Prozent) der Meinung, dass sie das Thema IT-Sicherheit eher gering bis überhaupt nicht betrifft."[23] Diese Ergebnisse überraschen, vor allem, wenn man bedenkt, dass mehr als drei Viertel der Befragten (76 Prozent) schon einmal von Viren, Trojanern, Abo-Fallen, Phishing oder Spyware betroffen waren.[24] Es steht ebenso im Gegensatz zu dem oben genannten Ergebnis, dass 90 Prozent der Befragten „[…] die Sicherheit von Dienstleistungen wichtig oder sehr wichtig ist […]".[25] Offensichtlich wurde die Gefahrensituation im Internet von der Bevölkerung erfasst. Jedoch scheint dies nicht zu dem gewünschten Ergebnis zu führen – der Wahrnehmung der Eigenverantwortung des mündigen Internetbürgers. Über die Gründe für ein solches Verhalten lässt sich nur spekulieren. Vermutlich ist zum Einen einfach der Schaden nicht groß genug, als dass ein angepasstes Verhalten erforderlich wäre.[26] Des Weiteren scheint der Aufwand, sich überhaupt mit dem Thema zu beschäftigen, eine Hürde darzustellen. Viele Menschen wissen möglicherweise nicht einmal, dass man sich mit einfachsten Vorsichtsmaßnahmen vor einem Großteil der Bedrohungen schützen kann.[27] Um letzteres positiv zu beeinflussen, ist ein anderer Umgang der Medien mit diesem Thema erforderlich. Bisher wird das Thema IT-Sicherheit nur bei spektakulären Ereignissen aufgegriffen und die Sachinformationen sind eher spärlich.

Der Themenkomplex IT-Sicherheit verteilt sich im Verhältnis zwischen Bürger und Staat über mehrere Ebenen. Die nachfolgenden Modelle sollen diese Ebenen und ihre Verknüpfungen untereinander verdeutlichen. Die Modelle erheben keinen Anspruch auf Vollständigkeit.

22 www.bsi-fuer-buerger.de

23 (Bundesamt für Sicherheit in der Informationstechnik, 2011) Bundesamt für Sicherheit in der Informationstechnik (2011). BSI-Bürgerumfrage zur Internetsicherheit: Internetnutzer in Deutschland schützen sich unzureichend vor bekannten Risiken. https://www.bsi.bund.de/cln_165/ContentBSI/Presse/Pressemitteilungen/Presse2011/BSI-Buergerumfrage-Internetsicherheit_11022011.html;jsessionid=8D465998FE22133C8C524095A26B8C1C (11.09.2011).

24 Ebd.

25 Ebd.

26 Das Bewusstsein für den sicheren Umgang mit Kontoinformationen ist weder auf der Seite der Nutzer noch auf der Seite der Banken vorhanden. Für die Banken ist es sinnvoller und ökonomischer, den individuellen Schaden der Nutzer zu ersetzen, als die Sicherheitsvorkehrungen zu erhöhen. Für den Nutzer entsteht kein finanzieller Schaden, wenn bspw. seine Kreditkarteninformationen missbraucht werden, da die Bank meist alle dadurch entstehenden Kosten übernimmt und dem Kunden das verlorene Geld ersetzt.

27 In der Studie des BSI wird ebenfalls erwähnt, dass die Zahl der installierten Anti-Virus-Programme rückläufig ist.

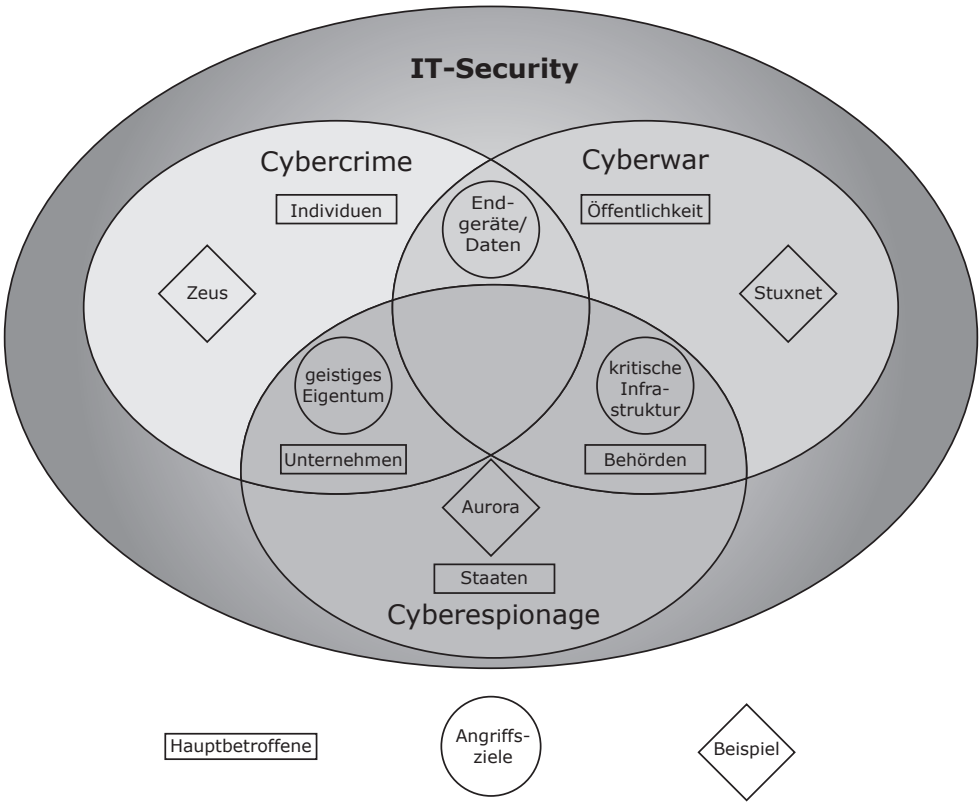


Abb. 1: IT-Sicherheit auf gesellschaftlicher Ebene

In den Modellen wird die gesellschaftliche Ebene der IT-Sicherheit in die drei Ebenen Cybercrime, Cyberwar und Cyberespionage aufgeteilt.[28] In allen Bereichen gibt es Überschneidungen und enge Verzahnung. Die angeführten Beispiele sind jeweils exemplarisch, bspw. ist bei einem Cyberkrieg auch immer der Staat betroffen, insbesondere, wenn sich dieser gegen Behörden richtet. Auf den Bereich der kritischen Infrastruktur wird unter Kapitel 2.3 noch gesondert eingegangen. Diejenigen, die am häufigsten betroffen sind – Unternehmen und Individuen – werden selten von der Öffentlichkeit wahrgenommen. Die vom Bundeskriminalamt (BKA) erfasste Computerkriminalität stieg im Jahr 2010 um 12,6 Prozent auf ca. 84.000 Fälle.[29] Auch im Bereich der Straftaten mit dem Tatmittel „Internet" verzeichnet das BKA einen deutlichen Anstieg, dabei handelt es sich in ca. 80 Prozent der Fälle um Betrugsdelikte.[30] In der Medienanalyse unter Kapitel 2.3 wird aber deutlich, dass diese Fälle in der Öffentlichkeit kaum wahrgenommen werden. Diese Art der Kriminalität lässt sich dauerhaft nur durch ‚Awareness' bekämpfen. Hierbei handelt es sich um ein

28 Dabei beruhen die Komponenten des noch sehr jungen Bereichs des Cyberkrieges auf Schätzungen. Diesem Bereich kann bisher nur ein Angriff überhaupt mit ziemlicher Sicherheit zugerechnet werden – *Stuxnet* – weshalb insbesondere die technische Ebene schwer einzuschätzen ist.

29 Bundeskriminalamt (2011). Polizeiliche Kriminalstatistik 2010, Bundesrepublik Deutschland. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/PKS2010.pdf?__blob=publicationFile (30.11.2010), S. 248.

30 Ebd. S. 255.

	Cybercrime	Cyberwar	Cyberspionage
Kosten pro Angriff	gering	sehr hoch	mittel
Schaden pro erfolgreichem Angriff	gering	sehr hoch	mittel
Häufigkeit der Angriffe	sehr hoch	sehr gering	mittel
Öffentliche Aufmerksamkeit	gering	sehr hoch	gering/mittel

Tabelle 1: Kosten und Häufigkeit von Cyberangriffen

Konzept, dass auf Aufklärung und Information setzt. Da sich gerade in Bereich der IT-Sicherheit die technischen Gegebenheiten sehr schnell ändern, ist vor allem ein Bewusstsein für die Gefahren und ihre Abwehr nötig. Erst dieses Bewusstsein führt bspw. zu regelmäßigen Softwareupdates und einer Installation von Anti-Virus-Software. Dass es zurzeit an ‚Awareness' in der Bevölkerung fehlt, zeigen die oben angeführten Ergebnisse der BSI-Umfrage. Da aber häufig die Endgeräte bzw. der Nutzer selbst betroffen sind, ist dies die einzige Möglichkeit die immensen materiellen Schäden, die damit einhergehen, nachhaltig zu reduzieren.

Betrachtet man die Tabelle fällt auf, dass die Häufigkeit der Angriffe in keinem Verhältnis zur öffentlichen Aufmerksamkeit steht. Spionage im Bereich kleiner und mittlerer

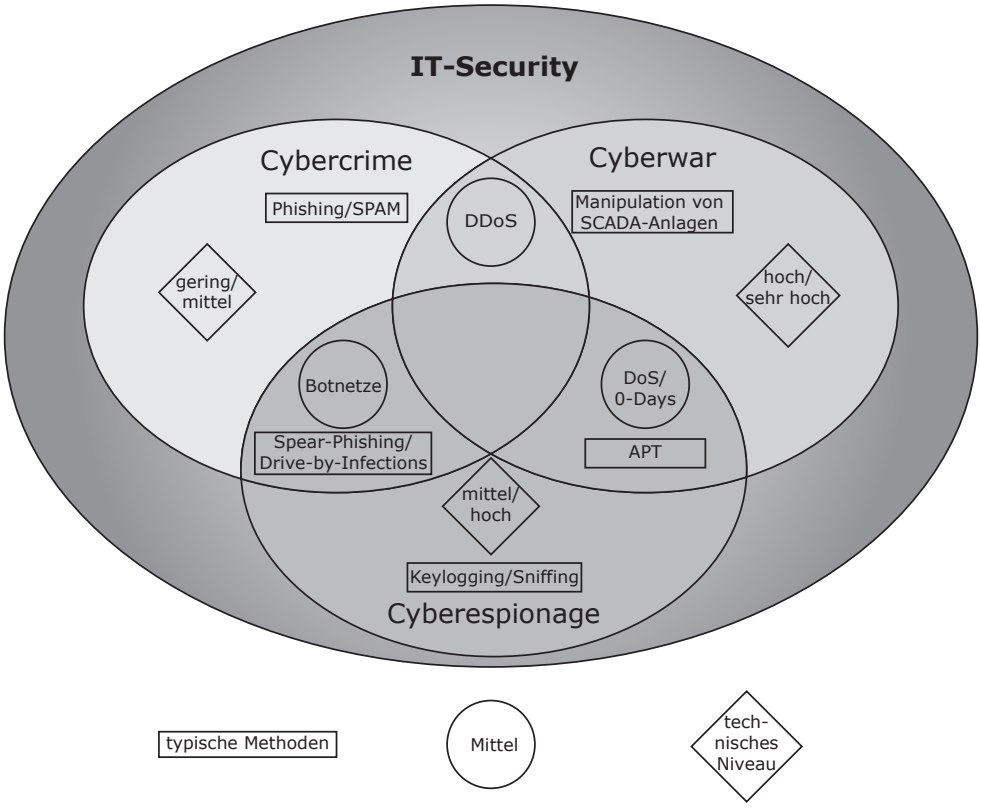


Abb. 2: IT-Security auf technischer Ebene

Unternehmen wird selten thematisiert, obwohl auf der Auswertung und Unterstützung bei der Abwehr solcher Angriffe ein Schwerpunkt des Nationalen Cyber-Abwehrzentrums der Bundesregierung liegen soll. Diese Fokussierung erscheint sinnvoll, da der Schaden, der durch Cyberespionage-Angriffe entsteht, für ein Unternehmen existenzbedrohend sein kann. Im Bereich des Cyberkriegs sind die Kosten eines Angriffs sehr hoch, da die Software für jeden Angriff einzeln entwickelt werden muss. Cyberkriminalität hingegen stellt den größten Anteil der Cyberangriffe dar. Durch die Häufigkeit der Angriffe entsteht in diesem Bereich der größte Gesamtschaden, obwohl ein einzelner Angriff mit geringem Aufwand realisiert werden kann. Dies ist auf technischer Ebene begründet.

Das Know-how der Angreifer im Bereich der Cyberkriminalität muss nicht besonders groß sein, um zum Erfolg zu führen. Die Struktur, die man für einen Angriff braucht, kann man für geringe Kosten im Internet mieten, bspw. Botnetze. Dies steht im Gegensatz zum Mitteleinsatz bei einem Angriff im Bereich des Cyberwars. Im Falle des bisher bekannten Angriffs, der definitiv dem Cyberkrieg zuzurechnen ist, sind sich die IT-Fachleute sicher, dass Stuxnet von einem Expertenteam entwickelt wurde.[31] Stuxnet ist somit einer relativ neuen Art von Cyberangriffen, den APT (Advanced Persistant Threats) zuzurechnen. Gemeint sind komplexe, aufwändige Cyberangriffe mit Langzeitcharakter, die regelmäßig von einer Gruppe durchgeführt werden. Einzelne Individuen verfügen nicht über die nötigen finanziellen und zeitlichen Ressourcen sowie das erforderliche Know-how. Es gibt aber eine Tendenz auch hinter solchen Angriffen stehenden Gruppen als APT zu bezeichnen. Die öffentliche Aufmerksamkeit bei solchen Angriffen ist aufgrund ihrer Seltenheit auch deutlich höher.

In diesem Kapitel wurde versucht einen groben Überblick über das komplexe Feld der IT-Sicherheit zu geben. Es besteht eine Verzahnung zwischen der gesellschaftlichen, der technischen und der materiellen Ebene, andererseits überlappen sich aber auch die Felder Cyberkriminalität, Cyberspionage und Cyberkrieg in mehrfacher Hinsicht. Die öffentliche Wahrnehmung konzentriert sich auf die gesellschaftliche Ebene, welche sich aber ohne technische Kenntnisse dem Verständnis entzieht. Auch hier sollte das Konzept der ‚Awareness' ansetzen, das die Bevölkerung über die Risiken, die mit der neuen Informationstechnologie einhergehen, umfassend informiert. Ein Mittel dazu könnten die Medien sein, die das Thema seit relativ kurzer Zeit für sich entdeckt haben, wie im folgenden Kapitel dargestellt wird.

2.3 IT-Sicherheit in der öffentlichen Wahrnehmung durch die Medien

Mediale Aufmerksamkeit wird nicht dadurch generiert, dass der Nutzer betroffen ist, sondern dadurch, dass es eine Story gibt. Eine Story muss bestimmten Regeln folgen, wenn sie erfolgreich sein will. Aus vielen kleinen Ereignissen, die immer wieder stattfinden, entsteht keine so gute Story, wie aus einem singulären Ereignis. Dies lässt sich gut nachvollziehen an der Medienaufmerksamkeit, die dem als *Millenium-Bug* oder *Y2K-Problem* bekannten Softwareproblem im Jahr 1999 gewidmet wurde. Im Gegensatz dazu ist der Trojaner *Zeus* den wenigsten ein Begriff, obwohl er mehrere Millionen Rechner infiziert hat und durch den Diebstahl von Bankdaten mindestens 70 Millionen Dollar Schaden

31 Kaspersky Lab (2010). Büchse der Pandora: Stuxnet läutet das Zeitalter der Cyberkriegsführung ein. http://www.kaspersky.com/de/news?id=207566394 (30.11.2011).

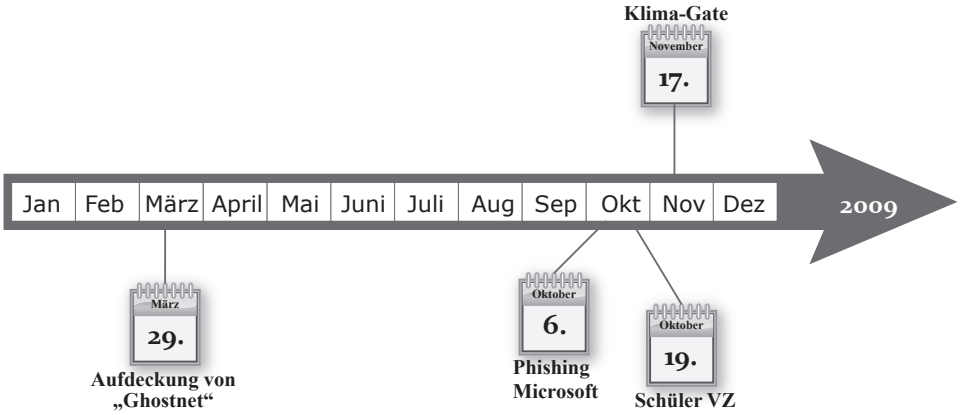


Abb. 3: Cyberangriffe und Spionage im Jahr 2009

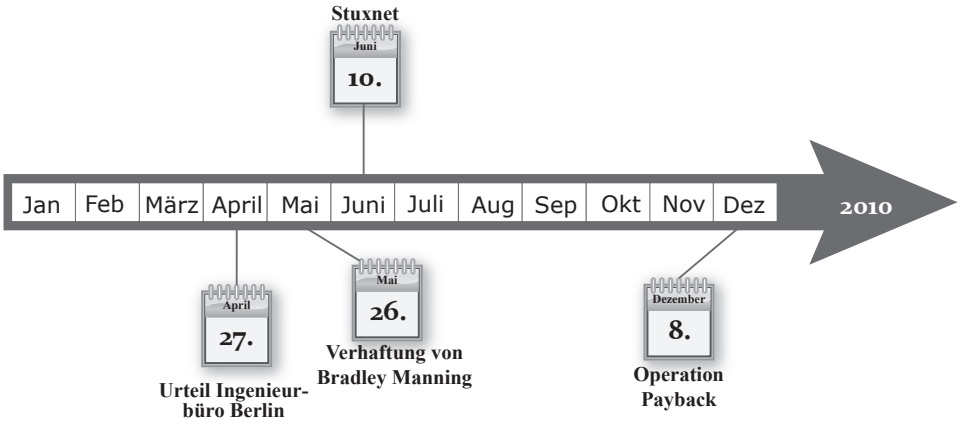


Abb. 4: Cyberangriffe und Spionage im Jahr 2010

verursacht hat. Zudem war und ist *Zeus* über eine lange Zeit aktiv (bekannt wurde er 2007), trotzdem war die mediale Aufmerksamkeit eher gering.

Allerdings ist im Verlauf der letzten drei Jahre ein bemerkenswerter Anstieg in der medialen Wahrnehmung von Themen zu verzeichnen, die die IT-Sicherheit betreffen. Es scheint, als ob das Bekanntwerden von *Stuxnet* einen Wendepunkt gebildet hätte. Die Möglichkeit eines Cyberkriegs wurde zum ersten Mal real. Durch die ausführliche und anhaltende Darstellung in den Medien ist der Öffentlichkeit die Rolle, die die Informationsinfrastruktur in der modernen Gesellschaft einnimmt, bewusster geworden und – damit einhergehend – auch deren Angreifbarkeit und die Abhängigkeit von dieser Infrastruktur. Dies hat zu einer anderen Wahrnehmung von IT-Sicherheit in der Öffentlichkeit geführt. Ein Indiz dafür ist die Anzahl der Ereignisse, über die in den Medien berichtet wird. Die folgenden Abbildungen[32] sollen

32 Die folgenden drei Abbildungen sind eine eigene Darstellung beruhen aber auf der Präsentation von René Klink „Aktueller Bericht aus der Praxis des Verfassungsschutzes“ vom Verfassungsschutz Berlin am „Tag der Unternehmenssicherheit“ der

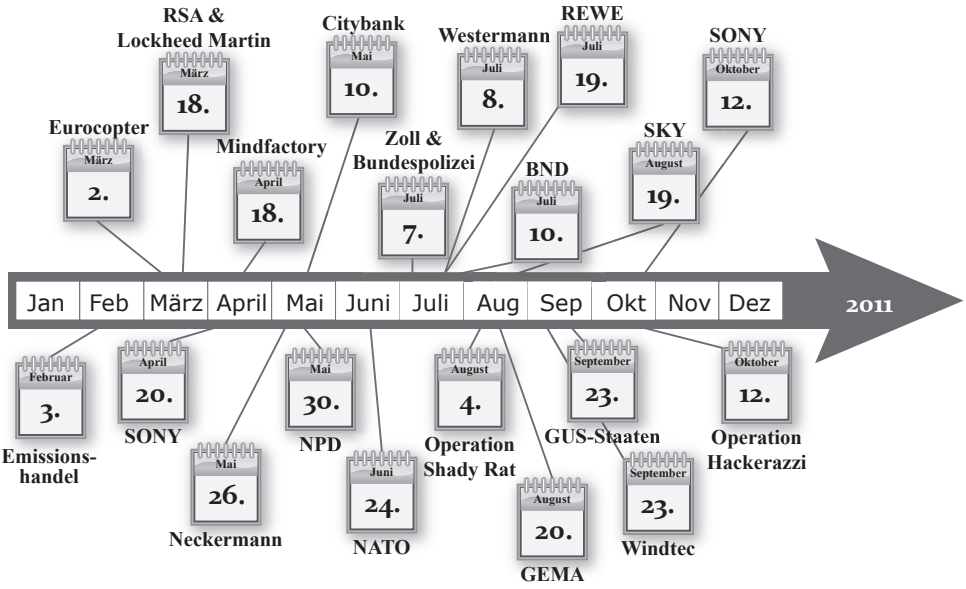


Abb. 5: Cyberangriffe und Spionage im Jahr 2011

dazu einen Überblick bieten, es wird kein Anspruch auf Vollständigkeit erhoben:

Als Hintergrundinformation zu den Abbildungen ist zu ergänzen, dass auch die Motivation der Taten bei der Bewertung durch den Verfassungsschutz Berlin eine Rolle spielt. Von den insgesamt 27 aufgeführten Ereignissen werden 15 (davon zwei nur zum Teil) als finanziell motiviert vom Verfassungsschutz bewertet. Ein staatlicher Angreifer wird bei sieben Fällen vermutet, ist im Einzelfall jedoch schwer nachweisbar. Die dritte Motivation ist politischer Natur (sieben Fälle). Diese ist häufig am eindeutigsten, da Gruppen wie Anonymus ihre Aktionen meist begründen. Bei einigen der angeführten Vorfälle kommt es zu Überschneidungen bei den vermuteten Motivationen. Die überwiegende Anzahl der bekanntgewordenen Angriffe sind finanziell motiviert.

Es ist deutlich zu erkennen, dass sich die öffentliche Wahrnehmung von IT-Sicherheitsthemen um ein Vielfaches gesteigert hat. Die öffentliche Meinung zu diesem Thema scheint sich derzeit im Wandel zu befinden. Da die Einstellungen, die daraus hervorgehen laut Page und Shapiro stabil sind und sich hauptsächlich aus den verfügbaren Informationen generieren, spielt die derzeitige mediale Darstellung der Themen zur IT-Sicherheit eine wichtige Rolle. Diese positive Entwicklung des Interesses an dem Thema kann genutzt werden, um die Vermittlung von Sachinformationen voran zu treiben. Denn bisher sind die Informationen eher auf ihre mediale Wirksamkeit ausgerichtet. Der mediale Fokus sollte sich vom Thema Cyberkrieg entfernen und einen Schwerpunkt auf Kriminalität und den Schutz der Endgeräte legen und alle unter Kapitel 2.2 dargestellten Ebenen beleuchten. Selbst wenn öffentlich-rechtliche Sender sich mit dem Thema IT-Sicherheit auseinandersetzen, führt das zu einer Aufarbeitung, die eher auf die Sensation als auf die Information ausgerichtet ist, wie man am Bsp. der Arte-Dokumentation „Vom

IHK Berlin am 19. Oktober 2011.

Digitalangriff zum Cyberkrieg“ deutlich erkennen kann.[33] Fernsehformate, die sich mit den neuen Medien auseinandersetzen und auch über sicherheitsrelevante Themen berichten, sucht man in Deutschland vergeblich.[34] Auch im Printbereich findet – abgesehen von Fachzeitschriften – so gut wie keine Information des Bürgers statt. Dies ist insofern unverständlich, als dass es sich beim Internet um eine Schlüsseltechnologie[35] handelt und die gesamte Gesellschaft auf eine funktionierende IT-Struktur angewiesen ist. Hier muss ein Umdenken stattfinden, damit die Bevölkerung auf breiter Ebene sachlich informiert wird und auf mögliche Risiken und die dazugehörigen Schutzmaßnahmen vorbereitet wird.

> „Mit dem Internet werden erstmals auch normale Bürger unmittelbare Akteure des Infrastrukturschutzes, und ihr Verhalten entscheidet mit über den Erfolg oder das Versagen von CIIP-Maßnahmen [Anm. d. A.: CIIP steht für Critical Information Infrastructure Protection].“[36]

Diese von Fischer identifizierten Akteure sind aber nicht auf ihre Rolle und die Situation insgesamt vorbereitet. Übungen wie die LÜKEX-Übung 2011 sind zwar ein erster Schritt, informieren aber nicht die Bevölkerung, sondern nur die Behörden. Eine Aufklärung der Bevölkerung ist beim Themenkomplex der IT-Infrastruktur aber eine notwendige Maßnahme, die bisher zum Teil der Interpretation durch die Medien überlassen wird und zum weitaus größeren Teil nicht stattfindet. Im Moment steigt die öffentliche Wahrnehmung von IT-Sicherheits-Themen deutlich an, so dass es ein geeigneter Zeitpunkt wäre, die Bevölkerung auf ihre Rolle vorzubereiten.

3. Fazit

Gerade im Bereich der IT-Sicherheit sind staatliche Strukturen eng verbunden mit Unternehmen und den einzelnen Individuen. Die sicherheitspolitischen Auswirkungen der neuen Informationstechnologie finden auf unterschiedlichen Ebenen statt, wie die Abbildung 1 zeigt. Die Verknüpfungen zwischen den einzelnen Akteuren sind dabei vielfältig. Auch Staaten sind bspw. von Cyberspionage betroffen und die volkswirtschaftlichen Schäden, die dabei entstehen, betreffen alle Akteure. Deshalb ist es wichtig, dass eine gemeinsame Sensibilisierung bezüglich der IT-Sicherheit in der gesamten Gesellschaft vorangetrieben wird, zumal nicht nur die Dauer der Internetnutzung, sondern auch die Anzahl der Internetnutzer in Deutschland kontinuierlich ansteigt.[37] Eine umfassendere und verbesserte Risikokommunikation seitens der Behörden ist somit unumgänglich. Nur eine umfassend informierte Öffentlichkeit kann auf neue Bedrohungen wie den Cyberkrieg angemessen reagieren.

Die IT-Infrastruktur ist zu einer Schlüsseltechnologie geworden, die alle Bereiche der Gesellschaft umfasst. Die Risiken, die

33 Arte: Vom Digitalangriff zum Cyberkrieg. Ausstrahlung: 07.07.2011, 20:15 Uhr, Trailer: http://videos.arte.tv/de/videos/vom_digitalangriff_zum_cyberkrieg_ausschnitt_1_2_-3955768.html (09.10.2011).

34 Zuletzt wurde das „c’t magazin“ eingestellt. Siehe z. B.: http://www.hr-online.de/website/fernsehen/sendungen/ct_magazin2964.jsp?rubrik=2964 Die Berichterstattung beschränkt sich häufig auf das Thema Cyberkriminalität, z. B. bei Einkäufen im Internet, und ist eher punktuell.

35 Vgl. Fischer, 2007, S. 6. Fischer weist darauf hin, dass es sich nicht im engeren Sinne um eine Technologie handelt, da das Internet auf Software basiert, aber von der Öffentlichkeit so wahrgenommen wird.

36 Fischer, 2007, S. 51.

37 ARD – ZDF Onlinestudie (2011). http://www.ard-zdf-onlinestudie.de/index.php?id=325 (08.10.2011).

damit einhergehen, sind fast immer globaler Natur. Deshalb ist insbesondere in diesem Bereich eine klare sicherheitspolitische Agenda erforderlich. Die Vorratsdatenspeicherung ist nur ein Teil dieses Komplexes, der jeden Bürger betrifft. Eine sicherheitspolitische Debatte über den Umgang mit dieser neuen Technologie und ihren Möglichkeiten und Risiken findet in Deutschland derzeit nicht statt.

Die Wahrnehmung von IT-Sicherheit in der Öffentlichkeit befindet sich zurzeit in einem Veränderungsprozess. Dieser Wahrnehmung liegt eine ambivalente öffentliche Meinung zugrunde. Das Verständnis dafür, dass das Thema weite Teile der Bevölkerung betrifft, wächst zusehends. Die Einsicht in die Notwendigkeit, selbst aktiv zu werden, geht damit jedoch nicht zwangsläufig einher. Die wenigen empirischen Untersuchungen, die es hierzu in Deutschland gibt, legen den Schluss nahe, dass der Prozess der Meinungsbildung in der Öffentlichkeit gerade erst begonnen hat. Die Herausbildung von Werten und Einstellungen diesbezüglich ist noch im Werden begriffen. IT-Sicherheit ist mit Themen, die für die Bevölkerung relevant sind, verknüpft, wie z. B. Datenschutz, Kriminalität und den Überwachungsmaßnahmen des Staates sowie auch Sicherheitspolitik. Die vielfache Vernetzung in der Gesellschaft führt dazu, dass die IT-Infrastruktur nicht nur zu einer Schlüsseltechnologie geworden ist, sonder auch dazu, dass ihre Sicherheit zum einem Schlüsselthema in der Gesellschaft werden wird.

Autoreninfo

Kristin Krüger, M. A., ist seit Juni 2010 beim Brandenburgischen Institut für Gesellschaft und Sicherheit tätig. Sie hat Germanistik und Soziologie an der Universität Rostock studiert. Nachdem sie ihren Bachelor erlangt hatte, setzte sie ihr Studium an der Humboldt-Universität zu Berlin in der Fächerkombination Soziologie und Politikwissenschaft fort. Hierbei kristallisierte sich ihr besonderes Interesse an sicherheitspolitischen Fragen heraus. Zurzeit spezialisiert sie sich weiter in diesem Bereich durch ein zweites Masterstudium „Military Studies“ an der Universität Potsdam.