Ausarbeitung

Militärische Aspekte von Internetsicherheit in Deutschland

[redacted]

Militärische Aspekte von Internetsicherheit in Deutschland

Verfasser: [redacted]
Aktenzeichen: WD 2 – 3000 – 065/11
Abschluss der Arbeit: 4. April 2011
Fachbereich: WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe
Telefon: +[redacted]

Inhaltsverzeichnis

1. Einleitung

Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind gemäß „Cyber-Sicherheitsstrategie für Deutschland“ vom Februar 2011 „zu einer existenziellen Frage des 21. Jahrhunderts geworden“.[1] Eine Begrenzung der Kriegsführung auf das Gefechtsfeld kriegführender Nationen sei nach Auffassung von Experten „unter Globalisierungsbedingungen eher unwahrscheinlich.“ (Die) hochtechnisierten Formen des Krieges im Informationszeitalter basieren „auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischen Fähigkeiten.“[2] Nach Presseangaben hat China in seinem neuen Weißbuch den Begriff der Landesverteidigung um „Cyberspace“ erweitert.[3]

Vor diesem Hintergrund ordnet die Ausarbeitung das Thema der Cyber-Sicherheit ein in allgemeine, militärische und völkerrechtliche Aspekte Deutschlands und der NATO gefolgt von wesentlichen öffentlich gewordenen militärischen Cyber-Aktivitäten und einer diesbezüglichen perspektivischen Zusammenfassung.

2. Deutschland

2.1. Allgemein

Nach Auffassung der Bundesregierung solle die „Sicherheit im Cyber-Raum und der Schutz der kritischen Informationsinfrastrukturen […] auf einem hohen Niveau gewährleistet (werden), ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.“[4] Der Ursprung von Cyber-Gefährdung liege „sowohl im In- als auch im Ausland.“ Häufig könne „bei Angriffen weder auf die Identität noch auf die Hintergründe des Angreifers geschlossen werden. Kriminelle, terroristische und nachrichtendienstliche Akteure nutzen den Cyber-Raum als Feld für ihr Handeln und machen vor Landesgrenzen nicht halt. Auch militärische Operationen können hinter solchen Angriffen stehen.“ Aufgrund der verteilten Verantwortung von Staat, Wirtschaft und Gesellschaft werde „eine Cyber-Sicherheitsstrategie nur dann erfolgreich sein, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen.“ Gleiches gelte nach Auffassung der Bundesregierung „im internationalen Kontext.“[5] Selbstkritisch stellt die Bundesre-

---

[1] „Cyber-Sicherheitsstrategie für Deutschland“, Internetportal Bundesministerium des Inneren, S. 2 f., Definitionen S. 14 f., URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile [01.03.2011].

[2] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung“, Konrad-Adenauer-Stiftung, Analysen & Argumente, Ausgabe 89, März 2011, S. 4, URL: http://www.kas.de/wf/doc/kas_22194-544-1-30.pdf?110311134036 [28.03.2011].

[3] „Chinas Armee erhebt globalen Anspruch“, 01.04.2011, in: Die Welt, S. 7.

[4] „Cyber-Sicherheitsstrategie für Deutschland“, ebenda, S. 3 f.

[5] „Cyber-Sicherheitsstrategie für Deutschland“, ebenda, S. 14.

gierung auch fest, dass „ohne internationale Abstimmung von Strategien nationale Maßnahmen allenfalls Teilerfolge erzielen (können)“, da Deutschland „zu wenig Ressourcen (habe).“[6]

Die Bundesregierung gestalte ihre Cyber-Außenpolitik daher so, „dass deutsche Interessen und Vorstellungen in internationalen Organisationen wie den Vereinten Nationen, der OSZE, dem Europarat, der OECD und der NATO koordiniert und gezielt verfolgt werden.“ Dabei gehe „es auch um die Etablierung eines von möglichst vielen Staaten zu unterzeichnenden Kodex für staatliches Verhalten im Cyber-Raum (Cyber-Kodex), der auch vertrauens- und sicherheitsbildende Maßnahmen umfasst.“[7]

Die Bundesregierung stellt im Weiteren fest, dass noch vor wenigen Jahren so gut wie alle Cyber-Attacken nachweisbar kriminellen Ursprungs waren. Zuletzt häuften sich jedoch Angriffe, „die als Spionage oder Sabotageversuch mit politisch-strategischem Hintergrund deutbar sind.“ Sicherheitspolitisch werde hier Neuland betreten. Wie bei anderen modernen Bedrohungsformen (Terrorismus, Piraterie, asymmetrische Kriege und „failing states“) verliere das Territorialprinzip und damit die Grenzverteidigung ihre Relevanz. Innere und äußere Sicherheit würden verschmelzen und der Angreifer könne nicht mehr identifiziert werden.

Nach Auffassung der Bundesregierung und aller Mitgliedstaaten der NATO geschehen „Angriffe auf Computernetze immer häufiger, sind besser organisiert und kostspieliger, was den Schaden angeht, den sie staatlichen Verwaltungen, Unternehmen, Volkswirtschaften und potenziell auch Transport- und Versorgungsnetzen und anderer kritischer Infrastruktur zufügen. (Sie können) eine Schwelle erreichen, die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euro-atlantischen Raums bedroht.“[8]

Für diese Position liefert die Bundesregierung in ihrer „Cyber-Sicherheitsstrategie für Deutschland“ vom 23. Februar 2011 auch das konkrete definitorische Fundament:

- „*Globale Cyber-Sicherheit*“ sei „der anzustrebende Zustand der InformationsTechnologie (IT)-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind.“
- Der „*Cyber-Raum*“ sei „der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab.“
- „*Cyber-Sicherheit in Deutschland*“ sei „der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind.“ Diese Cyber-Sicherheit entstehe durch die Summe von geeigneten und angemessenen Maßnahmen. „*Militärischer Cyber-Sicherheit*“ betrachte hierbei „die Menge der militärisch genutzten IT-Systeme des deutschen Cyber-Raums.“

---

[6] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung“, ebenda, S. 5.

[7] „Cyber-Sicherheitsstrategie für Deutschland“, ebenda, S. 11.

[8] „Strategisches Konzept für die Verteidigung und Sicherheit der Mitglieder der Nordatlantikvertrags-Organisation“, ebenda, Ziffer 12

- Ein „*Cyber-Angriff*“ sei ein „IT-Angriff im Cyber-Raum, der sich gegen einen oder mehrere andere IT-Systeme richtet und zum Ziel hat, die IT-Sicherheit zu brechen.“
- „*Cyber-Spionage*“ seien „Cyber-Angriffe, die sich gegen die Vertraulichkeit eines IT-Systems richten, wenn sie von fremden Nachrichtendiensten ausgehen oder gesteuert werden.“
- „*Cyber-Sabotage*“ seien „Cyber-Angriffe gegen die Integrität und Verfügbarkeit eines IT-Systems.“
- „*Kritische Infrastruktur*“ seien „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ Auf Bundesebene gäbe es dazu folgende Sektoreneinteilung: „Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung, Medien und Kultur.“[9]

2.2. Militärische Aspekte

„Cyber-War“ wird in der „Cyber-Sicherheitsstrategie für Deutschland“ nicht ausdrücklich definiert. Die Bundesregierung hat sich jedoch hierzu geäußert, so u.a., dass im Fall kriegerischer Auseinandersetzungen die elektronische Kampfführung über den virtuellen Raum mit Mitteln der Informationstechnik eine Schlüsselrolle spiele. Die hochtechnisierten Formen des Krieges im Informationszeitalter basierten auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischen Fähigkeiten. Eine Begrenzung der Kriegsführung auf das Gefechtsfeld kriegführender Nationen sei „unter Globalisierungsbedingungen eher unwahrscheinlich.“[10] Ungeachtet der Tatsache, dass zivile Ansätze und Maßnahmen bei der Cyber-Sicherheitsstrategie im Vordergrund stünden, würden diese „ergänzt durch die Maßnahmen der Bundeswehr zum Schutz ihrer eigenen Handlungsfähigkeit, um auf diese Weise Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge zu verankern.“[11]

Die Bundeswehr stellt selbst fest, dass „neue Bedrohung durch Cyber-Attacken, die auch die Bundeswehr direkt treffen können, ein radikales Umdenken – insbesondere der Militärs (erfordert).“ Traditionelle Konzepte und klassisches militärisches Schutzdenken würden nicht mehr greifen. Das läge zum einen „an der extremen Asymmetrie zwischen Angreifer und potenziellem Schaden“. 2010 hätte das Pentagon 14 Monate gebraucht, um den Wurm agent.btz unschädlich zu machen. Die Rückverfolgungsproblematik würde verstärkt durch die verschiedenen Möglich-

[9] „Cyber-Sicherheitsstrategie für Deutschland“, S. 14 f.

[10] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung“, Ebenda, S. 4.

[11] „Cyber-Sicherheitsstrategie für Deutschland“, S. 4 f.

keiten der Tarnung von Angriffen. „Das bipolare Denken von Angriff und Verteidigung funktioniert nicht mehr.“[12]

Das Bundesministerium der Verteidigung setzt für die Cyber-Sicherheit von Streitkräften zwei Institutionen unter seiner Führung ein:

- das „*Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr*“ zur Wahrung der Cyber-Verteidigung. Das Bundesamt realisiert nach eigenen Angaben „Projekte zur Ausstattung und Ausrüstung der Streitkräfte und der Wehrverwaltung mit aufgabengerechten, modernen und wirtschaftlichen IT-Verfahren und IT-Systemen.“ Es sei damit zentraler Dienstleister für die Streitkräfte und die Bundeswehrverwaltung. Dies umfasse „die Konzeption, die Analyse, die Projektierung und die Einführung sowie das Nutzungsmanagement.“ Das Bundesamt schaffe so „die Rahmenbedingungen für ein zeitgemäßes Informationsmanagement in der Bundeswehr“.[13]
- das „*Kommando Strategische Aufklärung*“[14] für das militärische Nachrichtenwesen einschließlich Cyber. Es soll nach Presseberichten 6.000 Soldaten umfassen und „durch Informationsgewinnung entscheidend zur militärischen Lagefeststellung und damit zur nationalen politischen Urteils- und Entscheidungsfähigkeit sowie zum Schutz der Soldatinnen und Soldaten im Einsatz bei (-tragen).“[15]

In einer jüngst erschienen Publikation der Bundeswehr wird die nationale Vorgehensweise im Falle eines Cyber-Angriffs anschaulich aufgezeigt: Für die Überwachung der eigenen Systeme sei der IT-Sicherheitsbeauftragte der Bundeswehr im IT-Amt zuständig. Sollten eine Dienststelle oder die Systeme im Einsatz Ziel eines Cyber-Angriffs durch Schadsoftware, wie zum Beispiel einen Virus oder Trojaner werden, würden die Sensoren beim „Computer Emergency Response Team“ der Bundeswehr (CERTBw) im IT-Zentrum in Euskirchen bei Bonn Alarm schlagen. Je nach Schwere des Sicherheitsrisikos werde der IT-Sicherheitsbeauftragte der betreffenden Dienststelle informiert und das CERTBw gäbe Gegenmaßnahmen vor. In besonders kritischen Fällen würde umgehend das „Risiko Management Board“ einberufen. Dieses entscheide über

---

[12] “Y”, das Magazin der Bundeswehr, 01.03.2011, URL: http://www.y-punkt.de/portal/a/ypunkt/aktuell/forschung_technik?yw_contentURL=/01DB131000000001/W28EJLJG737INFODE/content.jsp.html

[13] „Ist es 10 vor 12“, IT-Amt der Bundeswehr, URL: http://www.it-amtbw.de/portal/a/itamtbw/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9zJLE3BIgXZqUWhRfql-Q7agIAE5FDe0!/ [24.03.2011].

[14] „Kommando Strategische Aufklärung“, http://www.manfred-bischoff.de/KSA.htm [24.03.2011].

[15] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [28.03.2011].

alle weiteren Maßnahmen und koordiniere sie. Hierzu zähle auch die Anordnung, „Rechner vom Netz zu nehmen.“[16]

In den USA kooperiert die Bundeswehr nach Presseangaben mit dem „Cyber Command“, das zur Abwehr von Cyber-Angriffen auf Militärnetze zuständig und in Fort Meade bei der „National Security Agency“ angesiedelt ist. Das Bekenntnis zu „vernetzter Sicherheit” und einem „comprehensive approach” werde sich nach Expertenauffassung gerade im Feld der Cyber Security bewähren müssen.[17] Ebenfalls ist die Bundeswehr an dem „NATO Cooperative Cyber Defence Centre of Excellence“ in Tallinn beteiligt.[18]

2.3. Aspekte der Rüstungskontrolle

Mit Blick auf das Thema der Rüstungskontrolle und Abrüstung hegt die Bundesregierung Zweifel, ob der sich abzeichnende „Rüstungswettlauf” der Militärs und Nachrichtendienste im Bereich offensiver „Cyber War”-Fähigkeiten nicht doch frühzeitige kollektive Vertragskonstrukte erfordere. Nach den Erfahrungen mit dem Rüstungswettlauf im Nuklearwaffenbereich müsse dies „zumindest intensiv erörtert werden.“[19] Ergänzend wird darauf hingewiesen, dass der Generalsekretär der Vereinten Nationen, Ban Ki Moon, nach Presseangaben Anfang 2009 empfohlen hat, „Cyberwaffen künftig in der Liste der Massenvernichtungswaffen zu führen.“[20]

Nach Auffassung der Bundesregierung setze die USA vor Schaffung rechtlicher und institutioneller Instrumentarien für Cyber-Sicherheit auf internationalen Dialog über Verhaltensnormen und vertrauensbildende Maßnahmen, die wie im humanitären Völkerrecht später kodifiziert werden könnten. Internationale Vertragskonstrukte – z.B. ein „Cyber War Limitation Treaty” nach Vorbild der Rüstungskontrolle im Nuklearwaffenbereich („no first use” etc.) – würden nach Auffassung der USA als zu starr gelten, zu wenig verifizierbar und zu sehr auf staatliches Handeln fokussiert, um gegen asymmetrische Cyber-Bedrohungen effektiv wirken zu können. Lediglich im Bereich der Strafverfolgung sehe man gemeinsame Normen als sinnvoll an. Daher würden sich die USA entschlossen zeigen, „den in den Vereinten Nationen angestoßenen Dialog über Verhaltensnormen und vertrauensbildende Maßnahmen weiter voranzutreiben.“ Ein geeignetes Instrument wäre bei den Vereinten Nationen die Gruppe der Regierungsexperten (Group of Government Experts - GGE). […] Frühwarnsysteme in Form automatischer Sensorennetzwerke

---

[16] “Y”, das Magazin der Bundeswehr, 01.03.2011, URL: http://www.y-punkt.de/portal/a/ypunkt/aktuell/forschung_technik?yw_contentURL=/01DB131000000001/W28EJLJG737INFODE/content.jsp.html [31.03.2011].

[17] Ebenda.

[18] Homepage des “NATO Cooperative Cyber Defence Centre of Excellence”, URL: http://www.ccdcoe.org/ [28.03.2011].

[19] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung“, Ebenda, S. 5.

[20] „Das digitale Wettrüsten“, in: Süddeutsche Zeitung, 20.05.2009.

und Hotlines zwischen Staaten sollten ausgebaut werden. Deutschland werde „sich mit einer abgestimmten Cyber-Außenpolitik aktiv in diesen Diskussionsprozess einbringen."[21]

3. NATO

Das „Strategisches Konzept für die Verteidigung und Sicherheit der Mitglieder der Nordatlantikvertrags-Organisation" ist am 30. November 2010 in Lissabon mit dem Titel „Aktives Engagement, moderne Verteidigung" verabschiedet worden. Die 28 Staats- und Regierungschefs der Mitgliedstaaten stellen hierin fest, dass „Angriffe auf Computernetze … eine Schwelle erreichen (könnten), die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euroatlantischen Raums bedroht."[22]

Die Bundesregierung sieht die NATO in ihrer „Cyber-Sicherheitsstrategie für Deutschland" als „das Fundament transatlantischer Sicherheit" an. Die Allianz müsse „folgerichtig Cyber-Sicherheit in ihrem gesamten Aufgabenspektrum angemessen berücksichtigen". Die Bundesregierung befürworte „das Engagement des Bündnisses zugunsten einheitlicher Sicherheitsstandards, die die Mitgliedstaaten freiwillig auch für zivile Kritische Infrastrukturen übernehmen können, wie im neuen strategischen Konzept der NATO vorgesehen".[23] Die NATO könnte bei einem „vernetzten" Ansatz von militärischen und zivilen Anstrengungen auch als ein Organisator von gemeinsamen Anstrengungen im Feld der Cyber-Sicherheit fungieren. Dies würde die wichtige transatlantische Klammer hinsichtlich der Ressourcen schaffen.[24]

Weiter heißt es: „Wir werden gewährleisten, dass die NATO über das gesamte Spektrum an Fähigkeiten verfügt, die für die Abschreckung und Verteidigung gegen jede Bedrohung der Sicherheit unserer Bevölkerungen notwendig sind. Wir werden daher […] unsere Fähigkeit weiter entwickeln, Angriffe auf Computernetze zu verhindern, zu entdecken, sich dagegen zu verteidigen und sich davon zu erholen, auch indem wir den NATO-Planungsprozess dazu nutzen, nationale Fähigkeiten zur Bekämpfung der Computerkriminalität zu stärken und zu koordinieren, indem wir für alle NATO-Gremien einen zentralen Schutz vor Computerkriminalität gewährleisten und die Überwachungs-, Warn- und Reaktionsaufgaben der NATO im Bereich der Computerkriminalität besser mit denen der Mitgliedstaaten zusammenführen."[25]

---

[21] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung", ebenda, S. 5.

[22] „Strategisches Konzept für die Verteidigung und Sicherheit der Mitglieder der Nordatlantikvertrags-Organisation", http://www.bundesregierung.de/Content/DE/__Anlagen/2010/2010-11-30-neues-strategisches-konzept,property=publicationFile.pdf [24.01.2011].

[23] „Cyber-Sicherheitsstrategie für Deutschland", S 11.

[24] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung", ebenda, S. 5.

[25] „Strategisches Konzept für die Verteidigung und Sicherheit der Mitglieder der Nordatlantikvertrags-Organisation", ebenda, Ziffer 19.

Rund 3.000 Mitarbeiter habe die „NATO Communication and Information Systems Agency“ im Hauptquartier der Allianz im belgischen Mons. Dazu gehören 120 IT-Spezialisten, „die sich nur mit der Abwehr von Cyber-Attacken beschäftigen. Das „Cooperative Cyber Defence Centre of Excellence“ im estnischen Tallinn, in dem auch zwei deutsche Offiziere tätig sind, und die „Emerging Security Challenges Division“ beschäftigen sich mit der Grundlagenarbeit und organisieren Übungen und Konferenzen.“ [26]

4. Militärische Cyber-Aktivitäten

Im nachfolgenden werden öffentlich gewordene militärische Cyber-Aktivitäten in chronologischer Reihenfolge zusammengestellt, so wie sie sich in Presseartikeln und Foren im Internet finden. Hingewiesen wird ergänzend auf das Internetportal bundeswehr.de, wo sieben „Cyber-Angriffe“ im Zeitfenster 2001 bis 2009 aufgeführt werden.[27]

1990:
„Auch auf dem militärischen Schlachtfeld sollte die neue Technik bald Anwendung finden. Schon während des zweiten Golfkriegs 1990 gab es Planungen, eine Radarstation im Süden Iraks

[26] “Y”, das Magazin der Bundeswehr, 01.03.2011, URL: http://www.y-punkt.de/portal/a/ypunkt/aktuell/forschung_technik?yw_contentURL=/01DB131000000001/W28EJLJG737INFODE/content.jsp.html [31.03.2011].

[27] Internetportal „bundeswehr.de“, 01.03.2011, URL: http://www.y-punkt.de/portal/a/ypunkt/aktuell/forschung_technik?yw_contentURL=/01DB131000000001/W28EJMJC433INFODE/content.jsp [31.03.2011].

„Bekannte Cyber-Angriffe:

Code Red
07/2001: DDoS-Attacke legt Websites des Weißen Hauses zeitweise lahm.

Byzantine
Candor Ende 2002: Datendiebstahl in US-Militär- und Regierungsbehörden.

Estland
05/2007: Im „Web War I“ werden Websites der Regierung, von Zeitungen und Banken tagelang mit DDoS-Attacken lahmgelegt.

Ghostnet
2007-09: Angriff auf 103 Länder. Ziel: 1.295 Rechner von Botschaften und Regierungsbehörden.

Georgien
08/2008: Angriff auf georgische Regierungswebsites für mehrere Stunden.

Aurora
Mitte – 12/2009: Angriff auf die Rechner chinesischer Menschenrechtler und US-basierter Technologieunternehmen

Stuxnet
09/2010: Gezielter Angriff auf Siemens-Systemkomponenten unter anderem in iranischen Industrieanlagen.“

zu besetzen und von dort aus mit ‚Logikbomben' das irakische Luftabwehrsystem lahmzulegen."[28]

„Bei der Operation ‚Desert Storm' 1990 nutzten die Amerikaner den Cyberspace zur psychologischen Kriegführung. Militärhacker infiltrierten das interne Kommunikationssystem des irakischen Verteidigungsministeriums und verschicken Tausende E-Mails, in denen Saddams Offiziere vor einem Angriff gewarnt und aufgefordert wurden, sich zu ergeben. Die Rechnung ging auf: Einige irakische Kommandeure schickten ihre Soldaten vor dem Angriff in Urlaub, und zahlreiche Einheiten stellten ihre Panzer außerhalb der Militärbasen auf, sodass die Amerikaner sie leicht bombardieren konnten."[29]

1999:
„Während des Nato-Luftkrieges gegen Serbien 1999 war es der amerikanischen Luftwaffe durch einen elektronischen Trick gelungen, fiktive Flugzeuge in die Zielcomputer der serbischen Flugabwehr zu schleusen. Die serbischen Militärs verschossen ihre Abwehrraketen auf diese Phantomziele".[30]

„Die USA schalteten zudem mit ihren Computern teilweise die Stromversorgung und Kommunikationswege in Serbien aus."[31]

2003:
„Was digitale Offensivwaffen angeht, gibt sich das amerikanische Militär allerdings bedeckt, obgleich sie zweifellos existieren. Bekannt ist, dass die USA nach dem 11. September AlQaidas Finanz- und Rekrutierungsnetzwerk mit Viren infiltrierten. Sie konnten den Geldfluss der Terroristen teilweise verfolgen und Überweisungen von Finanziers der Gruppe auf Konten umleiten, die vom amerikanischen Militär kontrolliert wurden. 2003 soll das US-Militär auch ernsthaft überlegt haben, im Irak das komplette Internet lahmzulegen."[32]

---

[28] „Die @-Bombe", 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [28.03.2011].

[29] Ebenda.

[30] „Mit Schirm gegen Terror", 19.11.2010, in: die Tageszeitung, URL: http://www.taz.de/1/archiv/digitaz/artikel/?ressort=sw&dig=2010%2F11%2F19%2Fa0086&cHash=2c36b8ba0a [28.03.2011].

[31] „Zu Land, zu See, zu Luft und im Cyberspace", 19.11.2010, in: Frankfurter Rundschau, URL: http://www.fr-online.de/politik/zu-land--zu-see--zu-luft-und-im-cyberspace/-/1472596/4850664/-/index.html [28.03.2011].

[32] "Das digitale Wettrüsten", 20.05.2009, in: Süddeutsche Zeitung, URL: http://www.sueddeutsche.de/digital/cyberkrieg-das-digitale-wettruesten-1.451998 [28.03.2011].

2006:
„Al-Qaida droht US-Finanzbranche mit Hacker-Angriff.“[33]

2007:
„Einen Vorgeschmack auf diese Form der Kriegführung lieferte das israelische Militär bereits vor drei Jahren, beim Angriff auf eine geheime Baustelle in Syrien. Auf den Radarschirmen der syrischen Luftabwehr-Offiziere, die in den Morgenstunden des 6. September 2007 ihren Dienst taten, war kein Flugobjekts zu sehen, kein Warnsignal erklang, nichts: Friedliche Stille über Euphrat und Tigris.
Zur selben Zeit verging den Arbeitern auf einer geheimen Baustelle in Ostsyrien Hören und Sehen: Ein Blitz, Explosionen und kreischende israelische Eagle- und Falcon-Militärjets störten die Ruhe. Am Morgen wurde der Schaden des Angriffs deutlich: Die mit nordkoreanischer Hilfe entstehende Kernenergieanlage der Syrer war nur noch eine Ruine.
Während die syrischen Militärs sich über das Versagen ihres mehrere Milliarden Dollar teuren russischen Flugabwehrsystems ärgerten, feierte man in Israel den Erfolg einer neuen Art der elektronischen Kriegführung, des Cyberwar. Denn ihren Überraschungscoup verdankten die Israelis nicht etwa Bombern und Raketen, sondern Bits und Bytes. Israelische Militärhacker hatten in den Softwarecode des Netzwerks der syrischen Luftabwehr ‚Logikbomben‘ oder ‚Trojaner‘ genannte Programme eingeschmuggelt. Dank dieser Schadsoftware konnten die Israelis das gegnerische Luftabwehrsystem wie einen Zombie steuern. Während ihre Militärjets ihr Ziel fanden, hatte die syrische Luftabwehr eine friedliche Simulation auf ihrem Radar.“[34]

„Auch Sicherheitslücken und darauf aufsetzende Angriffsprogramme kaufen die Armeen dieser Erde gern bei gewöhnlichen Computerkriminellen ein. […] Für den im Jahr 2007 von mehr als 3500 PCs ausgeführten Angriff auf die informationstechnische Struktur Estlands sollen angeblich 25 000 Dollar an die privatwirtschaftlich organisierte IT-Tochter des weißrussischen Geheimdienstes KGB in Minsk geflossen sein.“[35]

„Chinesischen Militärs ist es einem Zeitungsbericht zufolge gelungen, Rechner des US-Verteidigungsministeriums zu infiltrieren. Ein Rechnersystem, das von Minister Gates' Büro genutzt wird, musste abgeschaltet werden. Der Vorfall habe in Verteidigungskreisen Sorge ausgelöst, dass China in ‚entscheidenden Momenten‘ die US-Systeme funktionsunfähig machen könnte.“[36]

---

[33] Al-Qaida droht US-Finanzbranche mit Hacker-Angriff“, 01.12.2006, in: Der Spiegel, URL: http://www.spiegel.de/wirtschaft/0,1518,451811,00.html [28.03.2011].

[34] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [28.03.2011].

[35] „Militärs suchen Strategien gegen Cyberattacken“, 15.02.2011, in: Frankfurter Allgemeine Zeitung, URL: http://www.faz.net/s/RubF3CE08B362D244869BE7984590CB6AC1/Doc~ED47780DE34374E4BA023E5558A7ECFC7~ATpl~Ecommon~Scontent.html [28.03.2011].

[36] „Chinesische Hacker legen Pentagon-Computer lahm“, 04.09.2007, in: Der Spiegel, URL: http://www.spiegel.de/netzwelt/web/0,1518,503678,00.html [28.03.2011].

2008:
„Als Modellfall künftiger Kriege gilt der Schlagabtausch 2008 zwischen Georgien und Russland um die abtrünnigen Gebiete Südossetien und Abchasien. Auch dort setzten Hacker Regierungsserver schachmatt. Das Besondere: Sie waren mit physischen Angriffen der russischen Armee koordiniert. ‚Die Attacken begannen größtenteils wenige Stunden vor den russischen Militäroperationen, und sie endeten kurz danach', stellte der US-Internet-Experte Scott Borg fest. Angriffsprogramme wurden zum Herunterladen über soziale Netzwerke verbreitet, einige Server und Botnetze waren zuvor von russischen kriminellen Organisationen benutzt worden."[37]

„Dass selbst das mächtigste Militär der Welt nicht sicher ist, haben jüngst die USA zugeben müssen. Ein Mitarbeiter hatte 2008 auf einem Stützpunkt im Nahen Osten einen verseuchten USB-Stick in einen Rechner gesteckt. Ein bösartiger Code, den ein Agent eines ausländischen Geheimdienstes darauf gespeichert hatte, bahnte sich unbemerkt einen Weg in die Rechner der US Central Command, das für die Kriege in Afghanistan und im Irak zuständige Regionalkommando der US-Streitkräfte. Das Virus spionierte vertrauliche Datenbanken aus und lieferte Informationen ins Ausland. US-Vizeverteidigungsminister William Lynn, der den Vorfall publik machte, bezeichnete ihn als ‚den bislang schwersten Einbruch in Systeme der US-Armee'."[38]

„Das Konzept des Cyberwar gewinnt zunehmend an Bedrohlichkeit, je stärker sich die industrialisierten Länder vernetzen. Im April 2008 drohte eine Qaida-Gruppe mit virtuellen Attacken gegen US-Atomkraftwerke und lieferte in einer Art offenen Brief gleich Belege des dafür nötigen Know-how. Der Angriff fand nie statt, die Echtheit der Drohung ist nicht verifiziert. Die technischen Möglichkeiten aber sind inzwischen unumstritten und werden auch genutzt."[39]

2009:
„Das Wall Street Journal berichtete im April 2009, Unbekannte seien in die Flugkontrolle der Luftwaffe ‚eingedrungen'. Die Zeitung berief sich auf Regierungsbeamte. Ein Geheimdienstoffizier warnte davor, dass ein Jagdflieger ‚seinem Radar nicht mehr vertrauen kann'."[40]

„Aber der Feind im Netz schläft nicht, wie die Attacke des Conficker-Wurms bewies, der im Februar 2009 mehrere Hundert Bundeswehr-Computer verseuchte."[41]

---

[37] „Der Feind im Netz", 15.03.2010, in: Focus, URL: http://www.focus.de/digital/computer/tid-17800/ausland-der-feind-im-netz-teil-2_aid_495306.html [28.03.2011].

[38] „Unsichtbare Angreifer", 23.09.2010, in: Süddeutsche Zeitung, URL: http://www.sueddeutsche.de/digital/kriegsfuehrung-im-cyberspace-unsichtbare-angriffe-mit-realen-folgen-1.1003586-2 [28.03.2011].

[39] „USA und Russland wollen virtuellen Rüstungswettlauf verhindern", 14.12.2009, in: Der Spiegel, URL: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,666880,00.html [28.03.2011].

[40] „Der Spion, der aus dem Cyberspace kam" vom 26.12.2010, in FAZ.NET, URL: http://www.faz.net/s/RubFC06D389EE76479E9E76425072B196C3/Doc~E2CFCE11426824B73A0981CE25C58CAD7~ATpl~Ecommon~Scontent.html [28.03.2011].

[41] Ebenda.

„Der F-35-Vorfall ist nur das neueste Glied in einer Kette von Cyber-Attacken gegen USA-Infrastruktur und -Rüstungseinrichtungen. Vor knapp zwei Wochen entdeckten Spezialisten in den Netzwerken der amerikanischen Stromnetzbetreiber unbekannte Programme, die möglicherweise dazu in der Lage gewesen wären, die US-Stromnetze abzuschalten. Zudem, so das ‚Wall Street Journal', sei das Luftüberwachungsnetz der US Air Force in den vergangenen Monaten Ziel von Internet-Attacken gewesen."[42]

„Das US-Militär will sogar ein zweites Internet bauen, National Cyber Range genannt, das als Testgelände für digitale Verteidigungs- und Angriffsmaßnahmen dient. Es wäre das elektronische Pendant zu einer militärischen Sperrzone wie das Bikini Atoll im Pazifik, auf dem die USA in den 1940er und 1950er Jahren Atomwaffen testeten. Mehrere Firmen haben im Januar den Auftrag erhalten, innerhalb von sechs Monaten erste Prototypen eines Testnetzes zu bauen, unter denen das Pentagon eines oder mehrere zur Weiterentwicklung auswählen wird."[43]

2010:
„ ‚Krieg wird heute mit Computern und Software ebenso geführt wie mit Panzern und Flugzeugen', sagt Hauptmann Christian Czosseck, einer von zwei deutschen Offizieren beim ‚Cooperative Cyber Defence Centre of Excellence' (CCDCOE) der NATO in Tallinn. Die Fähigkeit zum computergestützten, vernetzten Waffeneinsatz sei heute ein sehr wichtiges Element militärischer Überlegenheit. Manche Fachleute gehen schon so weit, den ‚Cyberspace' als das ‚fünfte Schlachtfeld' moderner Kriege zu sehen - nach Boden, Luft, Meer und Weltraum."[44]

„So ist es unbekannten Hackern schon gelungen, in die Datenbank des Bundeskanzleramts einzudringen und in E-Mail-Verzeichnisse des Weißen Hauses. Auch das Pentagon wurde ausgeforscht. Im vergangenen Jahr berichtete das ‚Wall Street Journal', unbekannte Spione hätten sich Zugang zu den Bauplänen des ‚Joint Strike Fighter' verschafft, des mit Tarnkappentechnik ausgestatteten Kampfflugzeugs F-35 ‚Lightning', welches die Zeitung als das ‚teuerste und technisch aufwendigste' amerikanische Waffensystem beschreibt."[45]

„Er verweist aber auf Presseberichte, denen zufolge es islamistischen Aufständischen schon einmal gelungen ist, amerikanische unbemannte Spionageflugzeuge zu beeinflussen. Sie hätten es zwar nicht geschafft, die Drohnen zu lenken, doch hätten sie Videos mitgeschnitten, welche die Drohnen an die amerikanische Bodenkontrolle funkten. ‚Alles, was aus der Ferne gesteuert werden kann, kann auch aus der Ferne missbraucht werden', sagt Czosseck."[46]

---

[42] „Hacker knacken geheimes Jet-Projekt", 21.04.2009, in: Der Spiegel, URL: http://www.spiegel.de/netzwelt/tech/0,1518,620208,00.html [28.03.2011].

[43] "Das digitale Wettrüsten", 20.05.2009, in: Süddeutsche Zeitung, URL: http://www.sueddeutsche.de/digital/cyberkrieg-das-digitale-wettruesten-1.451998 [28.03.2011].

[44] „Der Spion, der aus dem Cyberspace kam" vom 26.12.2010, ebenda.

[45] Ebenda.

[46] Ebenda.

„Am 4. Juli (2010) startete Pjöngjang eine massive Cyber-Attacke auf amerikanische und südkoreanische Webseiten. Unter dem virtuellen Ansturm von mehr als einer Millionen Anfragen pro Sekunde brachen die Webseiten der Landesschutzbehörde und der US-Regierung zusammen. Auch die Server von Transport- und Finanzministerium sowie des US-Geheimdienstes und der New Yorker Börse ließen die nordkoreanischen Hacker zwischen dem 4. und 9. Juli kollabieren. Lediglich das Weiße Haus blieb verschont, da der Internetverkehr rechtzeitig auf andere Server umgeleitet werden konnte.“[47]

„Aber auch die USA ziehen inzwischen in den virtuellen Krieg. US-Militärs etwa legen mit ihrem Luftangriffssystem ‚Suter‘ gezielt gegnerische Kommunikationssysteme lahm. Über eine Schadsoftware können die Amerikaner beispielsweise irreführende Daten als Phantomziele in feindliche Radarsysteme einspielen oder verfolgen, was der Gegner momentan auf seinem Radarschirm sieht. So kann die US-Luftwaffe kontrollieren, ob ihre Tarnkappen-Bomber ‚Stealth‘ tatsächlich unentdeckt bleiben.“[48]

„ ‚Das US-Militär wäre ohne das Internet genauso wenig arbeitsfähig wie Amazon.com‘, warnt Clarke“, der nach Presseangaben unter den US-Präsidenten Clinton und George W. Bush für Terrorismusabwehr zuständig und später Sonderberater für Cyber-Sicherheit im Weißen Haus war. „Die Vernetzung der Militärtechnik ist gleichzeitig die größte Achillesferse moderner Hightech-Rüstung. Viren und Würmer sind im Kampf David gegen Goliath eine gefährliche Waffe. […] Zwanzig bis dreißig weitere Staaten, darunter Russland, Südkorea, Indien, Pakistan, Frankreich und Israel, haben bereits schlagkräftige Online-Armeen aufgestellt.“[49]

„Von Anfang an setzten die Chinesen dabei auf einen Angriffskrieg im Cyberspace. Die Autoren einer 1999 erschienenen Strategieschrift des chinesischen Militärs verkünden unverhohlen ‚zhixinxiquan‘ oder Informationsvorherrschaft als Ziel eines solchen Konflikts: ‚Eine überlegene Streitmacht, die die Informationsvorherrschaft verliert, wird von einer unterlegenen besiegt werden, die diese gewinnt‘."[50]

„Offensive Mittel des Computerkriegs würden noch nicht intensiv untersucht, weil die Nato-Staaten darüber sehr unterschiedliche Vorstellungen hätten. Und Vergeltungsschläge seien kaum möglich, weil sich die Angreifer verstecken könnten und praktisch nicht zu identifizieren seien.“[51]

---

[47] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [28.03.2011].

[48] „Wikileaks ist erst der Anfang“, 07.12.2010, in: Wirtschaftswoche, URL: http://www.wiwo.de/technik-wissen/wikileaks-ist-erst-der-anfang-449150/4/ [28.03.2011].

[49] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, ebenda.

[50] Ebenda.

[51] „Der Spion, der aus dem Cyberspace kam“ vom 26.12.2010, in FAZ.NET, URL: http://www.faz.net/s/RubFC06D389EE76479E9E76425072B196C3/Doc~E2CFCE11426824B73A0981CE25C58CAD7~ATpl~Ecommon~Scontent.html [28.03.2011].

2011:
„Der britische Verteidigungsminister Nick Harvey plant sogar, abschreckende Online-Erstschlagkapazitäten aufzubauen. Künftig soll das britische Militär Kontrahenten mittels Cyber-Attacken erledigen können. Umgerechnet rund eine Milliarde Euro will Großbritannien in den nächsten Jahren für die Cyberwar-Vorbereitungen ausgeben."[52]

„In response to rising concerns over the vulnerability of national information and communication technology systems, many militaries are developing capabilities for assessing, countering and, presumably, prosecuting operations in cyberspace. But this again is a grey area: the boundaries between civil and military cyberspace are unclear, as is the role that the military should have in this realm. In a developing area with potential national security implications, it is perhaps unsurprising that militaries will seek to explore a potential role."[53]

Das Pentagon der USA finalisiert derzeit nach Presseangaben eine neue „Cyber Warfighting Strategy". Diese solle ein Rahmenwerk für Ausbildung und Ausrüstung als auch ein Aufruf für ein Mehr an internationaler Kooperation für Cyber-Sicherheit sein. Auch der Leiter des 2009 gegründeten US Cyber Command habe sich schriftlich im März diesen Jahres derart geäußert, dass seine strategische Initiative auf den Austausch von Informationen und eine Stärkung von „kollektiver Cyber-Sicherheit" zusammen mit Alliierten und internationalen Partnern ziele.[54]

5. Völkerrechtliche Aspekte

Robin Geiss, Völkerrechtler und Mitglied eines internationalen Expertengremiums, das mit Unterstützung der NATO an einem Handbuch zu Cyber-Attacken arbeitet, und der nach Pressangaben von 2007 bis 2010 Rechtsberater für das Internationale Komitee vom Roten Kreuz war, stellt fest: „Ob wir im Hinblick auf den Cyberspace bereits von Kriegen beziehungsweise von bewaffneten Konflikten im Rechtssinne sprechen können, ist mehr als zweifelhaft. Vieles von dem, was heute umgangssprachlich als Cyber-Angriff bezeichnet wird, löst noch lange keinen bewaffneten Konflikt im Sinne des Völkerrechts aus. […] Cyber-Attacken sind für viele Regierungen schon heute alltäglich. Die Informationsstrukturen der Nato werden täglich mehrfach attackiert. Die Frage ist: Ab wann erreichen diese Attacken eine solche Intensität, dass die Nato, wie bei einer militärischen Bedrohung, zum Gegenschlag ausholen darf? Etwa erst dann, wenn es in irgendeinem Kraftwerk kracht und funkt, die Cyber-Attacken sich also physisch auswirken? Oder muss das Völkerrecht nicht sagen: ‚Auch Attacken, die nur virtuell stattfinden, können heute schon dieselbe schreckliche Intensität erreichen'? […] Aber ich kann mir in der Tat militärische Szena-

[52] „Wikileaks ist erst der Anfang", 07.12.2010, in: Wirtschaftswoche, URL: http://www.wiwo.de/technik-wissen/wikileaks-ist-erst-der-anfang-449150/4/ [28.03.2011].

[53] "The Military Balance", Foreword, 08.03.2011, International Institute for Strategic Studies (IISS), URL: http://www.iiss.org/publications/military-balance/the-military-balance-2011/ [28.03.2011].

[54] „New Pentagon Cyber Strategy Complete: Official", 29.03.2011, in: DefenseNews, URL: http://www.defensenews.com/story.php?i=6092878&c=AME&s=TOP [31.03.2011].

rien vorstellen, wo Cyber-Attacken schonendere Angriffe ermöglichen als konventionelle Waffen. Cyber-Attacken können ja grundsätzlich auch reversibel gestaltet sein. Das heißt: Ich schalte ein Kraftwerk des Gegners aus - aber nur für drei Tage. Danach gehen die Lichter wieder an.“[55]

Die Völkerrechtlerin Katharina Ziolkowski arbeitet nach Presseangaben vom 1. April 2011 in Tallinn als Rechtsexpertin im „Cooperative Cyber Defense Center of Excellence“, dem renommierten Cyber-Sicherheit-Think-Tank der NATO. Ziolkowski lehrte zuvor an der Führungsakademie der Bundeswehr in Hamburg. 2010 hat sie die US-Armee beim „Centre for Law and Military Operations in Charlottesville” beraten. Ihr Buch „Praktische Probleme und Rechtsfragen bei Operationen im virtuellen Raum“ erscheint voraussichtlich 2011. Ihrer Auffassung nach gilt mit Blick auf Cyber-Sicherheit, dass „wann immer das humanitäre Völkerrecht den Schutz von Zivilisten, zivilen Objekten, der Umwelt und manchmal sogar des Gegners gebietet, kann man dies auch im Cyberspace weiter hochhalten.“ Im Weiteren heißt es in dem Artikel: „Die Haager Landkriegsordnung ist von 1907, die Genfer Konventionen von 1949, ihre zwei ersten Zusatzprotokolle von 1977, alles weit vor der Internet-Ära. Ich gehöre dennoch zu jenen, die meinen, dass die alten Regelwerke genügen und auch auf mögliche zukünftige Konflikte im Cyberspace anwendbar sind. Zumindest wenn wir nach Sinn und Zweck der einzelnen Regelungen fragen.“[56]

Nach Angaben der Bundeswehr sei „man sich nicht einig, ob ein digitaler Angriff nach internationalem Recht als ‚bewaffnet‘ gewertet werden soll. Auch die Tatsache, dass ein solcher schwer bis gar nicht zurückverfolgt werden kann“, erschwere die Ausübung des Rechts auf individuelle und kollektive Selbstverteidigung. „Wo kein Angreifer, da auch keine Verteidigung“.[57]

6. Zusammenfassung

Elf Jahre nachdem erste militärische Cyber-Aktivitäten öffentlich geworden sind, ist das Thema Cyber-Sicherheit auf der politischen Agenda angekommen und dies sowohl national als auch international. Handlungsnotwendigkeit der Staatengemeinschaft für Cyber-Sicherheit wird sichtbar zum einen durch die Erkenntnis, dass „jeder politische, wirtschaftliche oder militärische Konflikt einen Nebenschauplatz im Internet (hat).“[58] Und zum anderen auch durch das Bekenntnis der Bundeskanzlerin, Dr. Angela Merkel, dass „die Bedrohung nicht weniger gefährlich

[55] „Angriffe sind alltäglich“, 07.03.2011, in: die tageszeitung, URL: http://www.taz.de/1/netz/netzpolitik/artikel/1/angriffe-sind-alltaeglich/ [28.03.2011].

[56] „die Netzwerke der NATO werden ständig angegriffen“, 18.02.2011, in: sueddeutsche.de, URL: http://www.sueddeutsche.de/politik/2.220/cyber-sicherheit-die-netzwerke-der-nato-werden-staendig-angegriffen-1.1061631 [28.03.2011].

[57] “Y”, das Magazin der Bundeswehr, ebenda.

[58] „Die Militarisierung des Cyberspace“, 01.12.2010, in Neue Züricher Zeitung, S. 23.

als klassische militärische Angriffe (sei).“[59] Für Deutschland werden daher ab 1. April 2011 das Nationale Cyber-Abwehrzentrum und der Nationale Cyber-Sicherheitsrat seine Tätigkeit aufnehmen. Die 28 Staats- und Regierungschefs der NATO haben das Thema bereits im November 2010 prominent auf die Agenda gesetzt. Da auch die Vereinten Nationen eine globale Kultur für Cyber-Sicherheit seit 1993 fordern, müssten eigentlich die wichtigsten Voraussetzungen für internationale Fortschritte vorliegen.

Trotz des erkennbaren Willens der Staatengemeinschaft zweifeln Experten, dass Erfolge über nationale Maßnahmen hinaus für eine internationale Cyber-Sicherheit in Kürze erreicht werden können:

- Cyber-Sicherheit ist keine nationale Domäne und kann auch nicht durch nationale Hoheitsgewalt gewährleistet werden. Ganz im Gegenteil erlaubt es das Selbstverständnis des freien Internet, Einzelpersonen, Organisationen und auch Staaten diese Sicherheit regional oder global in ihrem Sinne temporär oder auf Dauer zu stärken oder zu mindern. Dabei stehen Staaten oftmals asymmetrische Akteure und Kosten gegenüber. Während sich ein einzelner Akteur die Leistungsfähigkeit weltweit verfügbarer privater Computer temporär kostenfrei für seine Absichten „aneignen“ kann, müsste von staatlicher und damit auch militärischer Seite ausschließlich mit eigenen Mitteln entgegengewirkt werden. Solange letzteres wie bisher nicht konzertiert von Staatengruppen erfolgt, könnte sich das Bild von David und Goliath zu Ungunsten von Staaten aufdrängen.
- Sandro Gaycken, der Technik- und Sicherheitsforscher an der Freien Universität Berlin, sieht für einen „wirksamen Schutz“ bei Cyber-Sicherheit drei Aspekte als Voraussetzung an: 1. Es müssen offensive Kapazitäten aufgebaut werden, „um Angriffe überhaupt im Detail verstehen zu können.“ 2. Der Selbstschutz müsse „radikal“ erhöht werden“ Und 3. Die „Abwehr von Sabotageakten“ müsse verstärkt werden. Der Experte stellt fest, dass hierfür „die zehn Stellen, die jetzt das Cyberabwehrzentrum in Bonn erhält“, sicher nicht ausreichen.[60]
- Verstärkt könnte die Schieflage von Staat zu Akteur auch durch den Tatbestand werden, dass das Völkerrecht Maßnahmen zur Durchsetzung von Cyber-Sicherheit noch nicht adäquat fördert. Auch hier steht die Staatengemeinschaft sichtbar und zögerlich erst am Anfang.
- Von Bedeutung ist die Definition von zentralen Begrifflichkeiten in der deutschen Cyber-Sicherheitsstrategie und damit auch was militärische Cyber-Sicherheit ausmacht. Voraussetzung für Erfolg ist ihre globale Anerkennung, um sie so zur Grundlage des gemeinsamen Handelns machen zu können. So wäre es durchaus möglich, neben euro-atlantischen Institutionen, wie NATO und Europäische Union, zusätzlich auch asiatische und afrikanische Organisationen in den Abstimmungsprozeß aufnimmt, so z.B. südostasiatische Nationen im Rahmen der ASEAN („Association of Southeast Asian Nations“) und die 53 Staaten der „Afrikanische Union“ einbezogen werden. Die Notwendigkeit hierfür als auch die Herkulesauf-

[59] “Merkel: Cyberwar so gefährlich wie klassischer Krieg”, 07.02.2011, in: Frankfurter Allgemeine Zeitung, URL: http://www.faz.net/s/RubDDBDABB9457A437BAA85A49C26FB23A0/Doc~EDB330E8D55AE42CFB27B83C8B9985309~ATpl~Ecommon~Scontent.html [28.03.2011].

[60] „Politik ist unglaublich schlecht beraten“, 31.03.2011, in: Die Welt, S. 8.

gabe an sich wird deutlich an der Tatsache, dass Cyber-Sicherheit stets nur so gut sein kann, wie das schwächste Glied in der globalen Kette.

- Optionen zur Cyber-Sicherheit hat die Münchner Sicherheitskonferenz Anfang Februar 2011 sowohl auf politischer als auch militärischer Ebene prominent diskutiert. Computerexperten waren sich gemäß Presseangaben einig, „dass es gegen digitale Angriffe nur ein wirksames Mittel der Verteidigung gibt, und zwar die rasche Veröffentlichung aller Sicherheitslücken, sowie sie bekannt werden." Die Diskussion in München hätte aber gezeigt, „dass eine internationale Übereinkunft zur Veröffentlichung von Sicherheitslücken, mit der dann die Entwicklung digitaler Angriffswaffen verhindert werden könnte, nicht in Sicht ist." Stattdessen scheine den Staaten „ein digitales Wettrüsten mit Cyberwaffen bevorzustehen, das eine gefährliche Dynamik anzunehmen verspricht."[61]

Nach Einschätzung von Experten wäre es durchaus möglich:

- dass sich die Staatengemeinschaft mittelfristig noch auf eine Zeit ohne ein internationales Regelwerk für Cyber-Sicherheit einstellt, da globale Vorstellungen noch zu deutlich divergieren. Nachvollziehbar wäre dies, wenn die Staaten bei gegenwärtigem status quo die Chancen des Cyber für staatliche Interessenswahrung höher einschätzen als die Risiken für eine solche. Wenn dies so ist, wird der von der Bundesregierung geforderte Kodex für staatliches Verhalten im Cyber-Raum (Cyber-Kodex), der auch vertrauens- und sicherheitsbildende Maßnahmen enthalten soll, noch auf sich warten lassen.
- dass die jetzige Lage es Staaten und Allianzen erleichtert, Erfolgsaussichten klassischer Einsätze von bewaffneten Streitkräften auch künftig durch Cyber-Maßnahmen zu befördern bzw. die anderer zu behindern. Militärische Einsatzplanungen, wie das „Internationale Institut für Strategische Studien" in seiner jüngsten „Military Balance 2011" feststellte, könnte somit ein erweitertes Aufgabenspektrum zugeschrieben werden. Die öffentlich gewordenen militärischen Cyber-Aktivitäten seit 1990, die von den USA in Kürze zu erwartende „Cyber Warfighting Strategy", das in den USA vorgesehene Testgelände für Cyber-Verteidigungs- und Angriffsmaßnahmen und das US-Luftangriffssystem „Suter" stützen diese Annahme. Die Schwelle zu kinetischen Angriffen könnte somit durch Cyber-Maßnahmen angehoben werden oder solche sogar ersetzen. In beiden Fällen würde diese Fähigkeit auch eine Kostenreduzierung von bewaffneten Einsätzen von Streitkräften bedeuten.

[redacted]

[61] „Militärs suchen Strategien gegen Cyberattacken", 15.02.2011, in: Frankfurter Allgemeine Zeitung, URL: http://www.faz.net/s/RubF3CE08B362D244869BE7984590CB6AC1/Doc~ED47780DE34374E4BA023E5558A7ECFC7~ATpl~Ecommon~Scontent.html [28.03.2011].