Wissenschaftliche Dienste

Deutscher Bundestag

Ausarbeitung

Nationale und internationale Maßnahmen zur militärischen Cyber-Sicherheit

[redacted]

WD 2 – 3000 – 076/11

Nationale und internationale Maßnahmen zur militärischen Cyber-Sicherheit

Verfasser: [redacted]
Aktenzeichen: WD 2 – 3000 – 076/11
Abschluss der Arbeit: 14. April 2011
Fachbereich: WD 2: Auswärtiges, Völkerrecht, wirtschaftliche Zusammenarbeit und Entwicklung, Verteidigung, Menschenrechte und humanitäre Hilfe
Telefon: +[redacted]

Inhaltsverzeichnis

1. Einleitung

Als „eine existenzielle Frage des 21. Jahrhunderts“ bewertet die „Cyber-Sicherheitsstrategie für Deutschland“ vom Februar 2011 die Verfügbarkeit des Cyber-Raums einschließlich der Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten.[1] Hochtechnisierte Formen des Krieges im Informationszeitalter basieren „auf einer weitgehenden Computerisierung, Digitalisierung und Vernetzung fast aller militärischen Fähigkeiten.“ Eine Begrenzung der Kriegsführung auf das Gefechtsfeld kriegführender Nationen sei daher „unter Globalisierungsbedingungen eher unwahrscheinlich.“[2]

Nach Auffassung der Bundesregierung bewerten die USA Cyber-Angriffe als vergleichbare Bedrohung wie z.B. die durch Nuklearwaffen in der Hand von Extremisten oder die durch eine Weiterverbreitung von Massenvernichtungswaffen und nuklearen Stoffen.[3] Nach Presseangaben finalisiert derzeit das Pentagon 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.[4] Das Bekenntnis zu „vernetzter Sicherheit” und einem „comprehensive approach” werde sich nach Expertenauffassung gerade im Feld der Cyber Security bewähren müssen.[5]

China hat nach Presseangaben in seinem neuen Weißbuch den Begriff der Landesverteidigung um „Cyberspace“ erweitert.[6]

Vor diesem Hintergrund beginnt die Ausarbeitung mit öffentlich gewordenen militärischen Cyber-Aktivitäten aus den Jahren 1990 bis 2011 gefolgt von Maßnahmen für Cyber-Sicherheit aus der Sicht Deutschlands, der Europäischen Union und der NATO. Völkerrechtliche und rüstungskontrollpolitische Aspekte gefolgt von einer perspektivischen Zusammenfassung runden das Thema ab.

---

[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 [14.04.2011].

[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 [15.04.2011].

[3] „Bericht der Bundesregierung zum Stand der Bemühungen um Rüstungskontrolle, Abrüstung und Nichtverbreitung sowie über die Entwicklung der Streitkräftepotenziale (Jahresabrüstungsbericht 2010)“, 27.11.2011, BT-Drucksache 17/4620, S. 54, URL: http://dip21.bundestag.btg/dip21/btd/17/046/1704620.pdf [14.04.2011]

[4] „New Pentagon Cyber Strategy Complete: Official“, 29.03.2011, in: DefenseNews, URL: http://www.defensenews.com/story.php?i=6092878&c=AME&s=TOP [14.04.2011].

[5] “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 [14.04.2011].

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

2. Militärische Cyber-Aktivitäten 1990 - 2011

Im nachfolgenden werden öffentlich gewordene militärische Cyber-Aktivitäten aus zwölf Jahren 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.[7]

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 zu besetzen und von dort aus mit ‚Logikbomben‘ das irakische Luftabwehrsystem lahmzulegen.“[8]

„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.“[9]

---

[7] Internetportal „bundeswehr.de“, 01.03.2011, URL: http://www.y-punkt.de/portal/a/ypunkt/aktuell/forschung_technik?yw_contentURL=/01DB131000000001/W28EJMJC433INFODE/content.jsp [14.04.2011].

„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.“

[8] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [14.04.2011].

[9] Ebenda.

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“.[10]

„Die USA schalteten zudem mit ihren Computern teilweise die Stromversorgung und Kommunikationswege in Serbien aus.“[11]

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.“[12]

2006:
„Al-Qaida droht US-Finanzbranche mit Hacker-Angriff.“[13]

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 Is-

[10] „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 [14.04.2011].

[11] „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 [14.04.2011].

[12] “Das digitale Wettrüsten”, 20.05.2009, in: Süddeutsche Zeitung, URL: http://www.sueddeutsche.de/digital/cyber-krieg-das-digitale-wettruesten-1.451998 [14.04.2011].

[13] 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 [14.04.2011].

raelis 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."[14]

„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."[15]

„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."[16]

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."[17]

„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 In-

[14] „Die @-Bombe", 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [14.04.2011].

[15] „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 [14.04.2011].

[16] „Chinesische Hacker legen Pentagon-Computer lahm", 04.09.2007, in: Der Spiegel, URL: http://www.spiegel.de/netzwelt/web/0,1518,503678,00.html [14.04.2011].

[17] „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 [14.04.2011].

formationen ins Ausland. US-Vizeverteidigungsminister William Lynn, der den Vorfall publik machte, bezeichnete ihn als ‚den bislang schwersten Einbruch in Systeme der US-Armee'."[18]

„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."[19]

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'."[20]

„Aber der Feind im Netz schläft nicht, wie die Attacke des Conficker-Wurms bewies, der im Februar 2009 mehrere Hundert Bundeswehr-Computer verseuchte."[21]

„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."[22]

„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

---

[18] „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 [14.04.2011].

[19] „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 [14.04.2011].

[20] „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 [14.04.2011].

[21] Ebenda.

[22] „Hacker knacken geheimes Jet-Projekt", 21.04.2009, in: Der Spiegel, URL: http://www.spiegel.de/netzwelt/tech/0,1518,620208,00.html [14.04.2011].

Auftrag erhalten, innerhalb von sechs Monaten erste Prototypen eines Testnetzes zu bauen, unter denen das Pentagon eines oder mehrere zur Weiterentwicklung auswählen wird.“[23]

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.“[24]

„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.“[25]

„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.“[26]

„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.“[27]

„Aber auch die USA ziehen inzwischen in den virtuellen Krieg. US-Militärs etwa legen mit ihrem Luftangriffssystem ‚Suter‘ gezielt gegnerische Kommunikationssysteme lahm. Über eine

---

[23] “Das digitale Wettrüsten”, 20.05.2009, in: Süddeutsche Zeitung, URL: http://www.sueddeutsche.de/digital/cyber-krieg-das-digitale-wettruesten-1.451998 [14.04.2011].

[24] „Der Spion, der aus dem Cyberspace kam“ vom 26.12.2010, ebenda.

[25] Ebenda.

[26] Ebenda.

[27] „Die @-Bombe“, 26.09.2010, in: Welt am Sonntag, URL: http://www.welt.de/die-welt/wissen/article9876810/Die-Bombe.html [14.04.2011].

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."[28]

„ ‚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."[29]

„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'."[30]

„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."[31]

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."[32]

„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

[28] „Wikileaks ist erst der Anfang", 07.12.2010, in: Wirtschaftswoche, URL: http://www.wiwo.de/technik-wissen/wikileaks-ist-erst-der-anfang-449150/4/ [14.04.2011].

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

[30] Ebenda.

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

[32] „Wikileaks ist erst der Anfang", 07.12.2010, ebenda.

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."[33]

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.[34] Nach Auffassung der Bundesregierung sehe der „Quadrennial Defense Review" der USA den weiteren Ausbau der Befähigungen im Cyberspace vor.[35]

3. Deutschland

3.1. 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."[36] 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."[37] Selbstkritisch stellt die Bundesregierung auch fest, dass „ohne internationale Abstimmung von Strategien nationale Maßnahmen allenfalls Teilerfolge erzielen (können)", da Deutschland „zu wenig Ressourcen (habe)."[38]

Die Bundesregierung gestalte ihre Cyber-Außenpolitik daher so, „dass deutsche Interessen und Vorstellungen in internationalen Organisationen wie den Vereinten Nationen, der OSZE, dem

---

[33] "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/ [14.04.2011].

[34] „New Pentagon Cyber Strategy Complete: Official", 29.03.2011, in: DefenseNews, URL: http://www.defensenews.com/story.php?i=6092878&c=AME&s=TOP [14.04.2011].

[35] Jahresabrüstungsbericht 2010, 27.11.2011, BT-Drucksache 17/4620, ebenda, S. 55.

[36] „Cyber-Sicherheitsstrategie für Deutschland", ebenda, S. 3 f.

[37] „Cyber-Sicherheitsstrategie für Deutschland", ebenda, S. 14.

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

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.“[39]

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.“[40]

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.“
- 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.“

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

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

- „*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.“[41]

3.2. Militärisch

„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.“[42] 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.“[43]

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 Möglichkeiten der Tarnung von Angriffen. „Das bipolare Denken von Angriff und Verteidigung funktioniert nicht mehr.“[44]

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 „Pro-

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

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

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

[44] “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 [14.04.2011].

jekte 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“.[45]

- das „*Kommando Strategische Aufklärung*“[46] 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).“[47]

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 alle weiteren Maßnahmen und koordiniere sie. Hierzu zähle auch die Anordnung, „Rechner vom Netz zu nehmen.“[48]

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.[49] Ebenfalls ist die Bundeswehr an dem „NATO Cooperative Cyber Defence Centre of Excellence“ in Tallinn beteiligt.[50]

---

[45] „Ist es 10 vor 12“, IT-Amt der Bundeswehr, URL: http://www.it-amtbw.de/portal/a/itamtbw/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9zJLE3BIgXZqUWhRfql-Q7agIAE5FDe0!/ [14.04.2011].

[46] „Kommando Strategische Aufklärung“, http://www.manfred-bischoff.de/KSA.htm [14.04.2011].

[47] „Die @-Bombe“, 26.09.2010, ebenda.

[48] “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 [14.04.2011].

[49] Ebenda.

[50] Homepage des “NATO Cooperative Cyber Defence Centre of Excellence”, URL: http://www.ccdcoe.org/ [14.04.2011].

4. Europäische Union

Die Bundesregierung beabsichtigt, auf Ebene der Europäischen Union geeignete Maßnahmen „aus dem Aktionsplan für den Schutz der kritischen Informationsinfrastrukturen (zu unterstützen).“[51]

Eine wesentliche Handlungsgrundlage auf der Ebene der 27 Mitgliedstaaten der Europäischen Union hat die Kommission zur „Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität […] vor Cyber-Angriffen und Störungen großen Ausmaßes“ bereits im März 2009 vorgelegt.[52] Die Kommission verweist hierin auf eine Schätzung des Weltwirtschaftsforums aus dem Jahr 2008, nach der „eine Wahrscheinlichkeit von 10 - 20 % (besteht), dass sich in den kommenden zehn Jahren ein größerer Ausfall der Informations- und Kommunikationstechnologien ereignen wird, der für die Weltwirtschaft Kosten von ca. 250 Mrd. US-Dollar verursachen könnte.“[53] Im Weiteren heißt es, dass kritische Informationsstrukturen „ein wichtiger Baustein der Innovation und für fast 40 % des Produktivitätsanstiegs verantwortlich (sei).“ Auch für die Arbeit von Regierungen und öffentlichen Verwaltungen seien diese „unverzichtbar“[54]. Ziel der Europäischen Kommission sei es daher, die „Europäische Agentur für Netz- und Informationssicherheit (ENISA) (zu stärken)“. Diese wurde „2004 geschaffen, um innerhalb der Gemeinschaft zu einer hohen und wirksamen Netz- und Informationssicherheit zum Nutzen der Bürger, Verbraucher, Unternehmen und Behörden beizutragen.“[55]

Mit Blick auf andere internationale Organisationen berücksichtigt die Europäische Kommission „Bemühungen der NATO für eine gemeinsame Politik zur Computerverteidigung, insbesondere im Rahmen der ‚Cyber Defence Management Authority‘ und des ‚Cooperative Cyber Defence Centre of Excellence‘.“ Schließlich werde „auch internationalen politischen Entwicklungen angemessen Rechnung getragen.“ [56] Hierzu zählt die Europäische Kommission:

- insbesondere die Grundsätzen der G8 für den Schutz kritischer Informationsinfrastrukturen,
- die Resolution 58/199 der Generalversammlung der Vereinten Nationen über die Schaffung einer globalen Kultur der Computer- und Netzsicherheit und den Schutz kritischer Informationsinfrastrukturen[57] sowie

---

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

[52] Kommission der Europäischen Gemeinschaften, „Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen“ vom 30.03.2009, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:DE:PDF [14.04.2011].

[53] Ebenda, S. 2.

[54] Ebenda, S. 4.

[55] Ebenda, S. 3.

[56] Ebenda, S. 4.

[57] „Creation of a global culture of cybersecurity and the protection of critical infrastructures“, Generalversammlung der Vereinten Nationen, URL: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf [14.04.2011].

- die jüngste Empfehlung der OECD über den Schutz kritischer Informationsinfrastrukturen.

Die Europäische Kommission warnt davor, dass „eine rein nationale Strategie die Gefahr von Uneinheitlichkeit und Effizienzverlust in sich (birgt).“ Von daher bedürfe „es einer gesamteuropäischen Anstrengung zur Verstärkung der nationalen Strategien und Programme.“[58] Vor diesem Hintergrund hat sie einen konkreten Aktionsplan mit konkreten Maßnahmen zur „Prävention und Abwehrbereitschaft“, „Erkennung und Reaktion“, „Folgeminderung und Wiederherstellung“, „Internationale Zusammenarbeit“ sowie „Kriterien für europäische kritische Infrastrukturen“ vorgelegt.

Ergänzend heißt es, dass „eine weitere Schwäche in der fehlenden Koordinierung der nationalen Ansätze hinsichtlich der Sicherheit und Robustheit der kritischen Informationsinfrastrukturen sowie in der unterschiedlich vorhandenen Fachkompetenz und Abwehrbereitschaft (liegt), was zu Uneinheitlichkeit und Effizienzverlust in Europa führt.“ Für die internationale Zusammenarbeit sei „es von wesentlicher Bedeutung, die Weltgemeinschaft in die Ausarbeitung einer Reihe von Grundsätzen für ein robustes und stabiles Internet, die die zentralen Werte Europas widerspiegeln, einzubeziehen, und zwar im Rahmen eines strategischen Dialogs und der Zusammenarbeit mit Drittländern und internationalen Organisationen.“[59]

Der Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu dem vorgenannten Papier der Europäischen Kommission ist zu entnehmen, dass „Europa nur sehr schlecht auf Cyber-Angriffe und Störungen großen Ausmaßes vorbereitet ist, da die Maßnahmen der einzelnen Mitgliedstaaten für den Schutz kritischer Informationsinfrastrukturen oftmals uneinheitlich und unzureichend koordiniert sind.“[60]

Im Weiteren stellt der Europäische Wirtschafts- und Sozialausschuss fest, dass „Regierungen und Anbieter grundlegender Dienste Sicherheits- und Stabilitätsprobleme nur publik (machen), wenn dies unausweichlich ist.“ Dennoch gäbe „es zahlreiche öffentliche Beispiele für die Bedrohung kritischer Infrastruktur durch Sicherheits- und Stabilitätsprobleme:

- Estland, Litauen und Georgien wurden 2007 und 2008 Opfer von Cyber-Großangriffen.
- Die Unterbrechung von Tiefseekabeln im Mittelmeer und im Persischen Golf führte 2008 zu Störungen des Internetverkehrs in zahlreichen Ländern.

---

[58] Kommission der Europäischen Gemeinschaften gemäß Fn. 28, S. 6.

[59] „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes“, Europäische Kommission, URL: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/si0010_de.htm [14.04.2011].

[60] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses zu der "Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen — "Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität" vom 22.09.2010, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:255:0098:01:DE:HTML [14.04.2011].

- Im April 2009 gaben die Sicherheitsbehörden der Vereinigten Staaten bekannt, dass Cyberspione in das US-Stromnetz eingedrungen sind und Softwareprogramme hinterlassen haben, die zur Störung des Systems benutzt werden könnten.
- Im Juli 2009 verzeichneten die Vereinigten Staaten und Südkorea eine DoS-Attacke[61] (mit 100000 bis 200000 ‚Zombie-Computern'), die zahlreiche Regierungs-Websites beeinträchtigte."[62]

Der Europäische Wirtschafts- und Sozialausschusses schließt sich „der in der Resolution 58/199 der UN-Generalversammlung erhobenen Forderung zur Schaffung einer globalen Kultur der Cyber-Sicherheit und Schutz kritischer Informationsinfrastrukturen an." Weiter heißt es, dass „angesichts der gegenseitigen Abhängigkeit der verschiedenen Länder in Bezug auf Sicherheit und Robustheit kritischer Informationsinfrastrukturen und der Tatsache, dass jede Kette nur so stark ist wie ihr schwächstes Glied, es besorgniserregend (ist), dass bislang lediglich neun Mitgliedstaaten so genannte Computer-Notfallteams (Computer Emergency Response Teams – CERT) eingerichtet haben."[63] Diese Computer-Notfallteams sollen, wie auch in der NATO, „umfassende nationale Risikomanagementverfahren und geeignete Präventionsmaßnahmen und -mechanismen aufstellen.[64]

Das Europäische Parlament hat Anfang März 2010 in einer Entschließung „zur Umsetzung der Europäischen Sicherheitsstrategie und der Gemeinsamen Sicherheits- und Verteidigungspolitik" festgestellt, dass die „Bedrohung der Computer- und Netzsicherheit" „die größte Bedrohung und Aufgabe" sei und forderte daher die Erstellung einer „Europäischen Strategie für Computer- und Netzsicherheit."[65]

5. 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

[61] DoS = Department of State.

[62] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, Ziffer 3.1.3.

[63] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, Ziffer 4.2.

[64] Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses, Ziffer 2.2.

[65] Bericht des Europäischen Parlaments vom 2. März 2010 über die Umsetzung der Europäischen Sicherheitsstrategie und der Gemeinsamen Sicherheits- und Verteidigungspolitik, URL: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2010-0026&language=DE [14.04.2011].

(könnten), die den Wohlstand, die Sicherheit und die Stabilität von Staaten und des euro-atlantischen Raums bedroht.“[66]

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“.[67] 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.[68]

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.“[69]

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.“ [70]

---

[66] „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 [14.04.2011].

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

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

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

[70] “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 [14.04.2011].

Nachfolgend werden in der Fußnote die auf der NATO-homepage dargestellte Cyber-Verteidigungspolitik und ihre diesbezüglichen Aktivitäten einschließlich der Evolution wiedergegeben.[71]

6. Aspekte der Rüstungskontrolle und des Völkerrechts

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."[72] 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."[73]

---

[71] "NATO´s Cyber Defence Policy and Activities, Context und Evolution", 18.03.2011, URL: http://www.nato.int/cps/en/natolive/topics_49193.htm [14.04.2011].

"Though NATO has always been protecting its communication and information systems, the 2002 Prague Summit included this function on the political agenda. Building on the technical achievements put in place since Prague, Allied leaders reiterated the need to protect these information systems at their Summit in Riga in November 2006.
A series of major cyber attacks on Estonian public and private institutions in April and May 2007 prompted NATO to take a harder look at its cyber defences. At their meeting in June 2007 Allied Defence Ministers agreed that urgent work was needed in this area. Pursuant to this agreement, NATO conducted a thorough assessment of its approach to cyber defence and reported back to Ministers in October 2007.
This report recommended specific roles for the Alliance as well as the implementation of a number of new measures aimed at improving protection against cyber attacks. It also called for the development of a NATO cyber defence policy.
Since the cyber attacks against Estonia in 2007, cyber threats have rapidly evolved in frequency and sophistication. In the summer of 2008, the war in Georgia demonstrated that cyber attacks have become a major component of conventional warfare. The development and use of destructive cyber tools that can threaten national and Euro-Atlantic security, represents a strategic shift that has increased the urgency for a new NATO cyber defence policy and a strengthening of defences.
Both the new Strategic Concept and the Lisbon Summit Declaration make clear that the rapid evolution and growing sophistication of cyber attacks make the protection of Allies' information and communications systems an urgent task of NATO on which its future security depends.
The 2010 NATO Lisbon Summit in particular has mandated development of a new NATO policy on cyber defence and an action plan by end June 2011 for its implementation.
NATO will use also its defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimize information sharing, collaboration and interoperability. Allies will also work to support the development of international norms of behaviour in cyberspace.
To address the security risks emanating from cyberspace, NATO will work closely with other actors, such as the UN and the EU."

[72] „Cyber-Sicherheit, Die Sicherheitsstrategie der Bundesregierung", Ebenda, S. 5.

[73] „Das digitale Wettrüsten", in: Süddeutsche Zeitung, 20.05.2009.

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 und Hotlines zwischen Staaten sollten ausgebaut werden. Deutschland werde „sich mit einer abgestimmten Cyber-Außenpolitik aktiv in diesen Diskussionsprozess einbringen."[74]

Ergänzend kündigt die Bundesregierung in ihrem Jahresabrüstungsbericht 2011 an, dass sie „als zunehmend wichtigem Thema auch für vertrauens- und sicherheitsbildende Maßnahmen (VSBM) verstärkte Anstrengungen der internationalen Abstimmung im Bereich IT-Sicherheit" ansieht. Von daher beteilige sie sich auch in den Vereinten Nationen „ aktiv an der VN-Regierungsexpertengruppe zu dem Thema und unterstützte zusammen mit den USA erstmals als Miteinbringer die von Russland eingebrachte Resolution zu internationalen Aspekten der IT-Sicherheit."[75] Als konkrete Aufgabe und Ziel für 2011 habe die Bundesregierung insbesondere: die „Erarbeitung und internationale Abstimmung internationalen Verhaltensregeln zu Cybersecurity" auf der internationalen Agenda gesetzt.[76]

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 Szenarien vorstellen, wo Cyber-Attacken schonendere Angriffe ermöglichen als konventionelle Waf-

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

[75] Jahresabrüstungsbericht 2010, ebenda, S. 6.

[76] Ebenda, S. 7 f.

fen. 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.“[77]

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.“[78]

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“.[79]

7. Deutscher Bundestag

Sowohl in der Öffentlichen Anhörung als auch in der Debatte des Deutschen Bundestages wurde das Thema der Cyber-Sicherheit wiederholt in Verbindung mit Artikel 4 und Artikel 5 des Washingtoner (NATO) - Vertrages vom 24. August 1949 gebracht. Der Wortlaut der Artikel wird daher nachfolgend wiedergegeben:[80]

Artikel 4

Die Parteien werden einander konsultieren, wenn nach Auffassung einer von ihnen die Unversehrtheit des Gebiets, die politische Unabhängigkeit oder die Sicherheit einer der Parteien bedroht sind.

---

[77] „Angriffe sind alltäglich“, 07.03.2011, in: die tageszeitung, URL: http://www.taz.de/1/netz/netzpolitik/artikel/1/angriffe-sind-alltaeglich/ [14.04.2011].

[78] „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 [14.04.2011].

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

[80] Der Washingtoner (NATO) - Vertrag, URL: http://www.asfrab.de/nato-vertrag.html [10.03.2011].

Artikel 5

Die Parteien vereinbaren, dass ein bewaffneter Angriff gegen eine oder mehrere von ihnen in Europa oder Nordamerika als ein Angriff gegen sie alle angesehen werden wird; sie vereinbaren daher, daß im Falle eines solchen bewaffneten Angriffs jede von ihnen in Ausübung des in Artikel 51 der Satzung der Vereinten Nationen anerkannten Rechts der individuellen oder kollektiven Selbstverteidigung der Partei oder den Parteien, die angegriffen werden, Beistand leistet, indem jede von ihnen unverzüglich für sich und im Zusammenwirken mit den anderen Parteien die Maßnahmen, einschließlich der Anwendung von Waffengewalt, trifft, die sie für erforderlich erachtet, um die Sicherheit des nordatlantischen Gebiets wiederherzustellen und zu erhalten. Von jedem bewaffneten Angriff und allen daraufhin getroffenen Gegenmaßnahmen ist unverzüglich dem Sicherheitsrat Mitteilung zu machen. Die Maßnahmen sind einzustellen, sobald der Sicherheitsrat diejenigen Schritte unternommen hat, die notwendig sind, um den internationalen Frieden und die internationale Sicherheit wiederherzustellen und zu erhalten.

7.1. Öffentliche Anhörung

Der Auswärtige Ausschuss hat am 6. Oktober 2010 eine öffentliche Anhörung zum neuen Strategischen Konzept der NATO durchgeführt. Im nachfolgenden werden hieraus wesentliche Argumente zum Thema der Cyber-Sicherheit sowohl der Abgeordneten als auch der geladenen Experten in chronologischer Reihenfolge aufgeführt.[81]

„Das neue Strategische Konzept wird die Kernaufgaben der NATO im 21. Jahrhundert beschreiben. Die Stichworte lauten: 11. September, grenzüberschreitender Terrorismus, nukleare Proliferationen, Cyber-Attacken, aber auch neue Partnerschaften, verbessertes Krisenmanagement und Stärkung der kollektiven Verteidigungsfähigkeit.“[82]

„Die Suche nach aktiven Aufgaben gestaltete und gestaltet sich allerdings als außerordentlich problematisch und schwierig. Einige dieser gegenseitig diskutierten Vorschläge, auch im Zusammenhang mit dem Strategischen Konzept sind offensichtlich ungeeignet. Hierzu gehören etwa Cybersicherheit als künftige Kernaufgabe der NATO.“[83]

„Die entscheidende Frage ist, glaube ich, tatsächlich jetzt auch oder auch für die nächsten Wochen noch, was konstituiert denn heute einen Art. 5-Fall. Der Generalsekretär hat sich zumindest ja mit dem, was in der Presse angedeutet worden ist, sehr weit aus dem Fenster gelehnt, dass sich diese Fragen von Cyber Security und Cyber-Attacken einem Art. 5-Fall annähern würden. Ich glaube, das ist eine Frage, die noch eine tiefere Betrachtung verdient und die man, glaube ich, auch sehr kontrovers diskutieren kann.[84] […] Und damit bin ich bei Cyber War. In der

[81] Deutscher Bundestag, Protokoll 17/20, 6. Oktober 2010, URL: http://www.bundestag.de/bundestag/ausschuesse17/a03/anhoerungen/prot17_20.pdf [10.03.2011].

[82] Ruprecht Polenz, MdB, ebenda, S. 2.

[83] Dr. Matthias Dembinski, Hessische Stiftung Friedens- und Konfliktforschung, ebenda, S. 2.

[84] Dr. Markus Kaim, Stiftung Wissenschaft und Politik, ebenda, S. 11.

Tat, ich halte auch nichts von dieser Gleichsetzung, Cyber War wäre das Äquivalent zu einem klassischen Angriff auf das Territorium der NATO. Erstens […]: diese Angriffe sind in der Regel deterritorial. Wir können den Urheber noch nicht einmal identifizieren. Da kann man noch sagen, da gab es einen Server irgendwie in Russland. Dahinter könnten aber auch Hacker in China stecken. Wir wissen es einfach nicht genau. Und […] wir können einen Beginn noch nicht einmal klar identifizieren. Wenn wir aber beides nicht können, wir können den Angreifer nicht identifizieren, um in den klassischen Kategorien zu sprechen, und wenn wir den Punkt des Angriffs nicht identifizieren können, damit ist eigentlich die Frage obsolet, ob wir eigentlich Art. 5 aktivieren können."[85]

„Wie also in diesen Fragen ein Militärbündnis tatsächlich stabilisierend wirkend kann, wird m.E. nicht hinreichend angesprochen, ganz zu schweigen von der Antizipation einer Ziel-Mittel-Relation für die neuen Probleme von Cyber-War bis Klimawandel, wie sie genannt werden.[86] […] Das Problem bei Cyber War besteht ja nicht nur darin, dass es schwer ist, diesen Fall als Angriff zu definieren, sondern auch die Verantwortung zuzurechnen. Es kann durchaus sein, dass der Staat, aus dem heraus ein solcher Angriff verübt wird, sich völlig rechtskonform verhält und überhaupt kein Interesse daran hat, dass private Akteure, die innerhalb seiner Grenzen agieren, genau dieses tun. Und die Frage ist, wo diskutiert man darüber? Ich denke, wenn man außerhalb der NATO darüber diskutiert, die UNO ist natürlich immer ein Forum, aber vielleicht wäre das auch ein Thema für die G-20. Ich meine, wenn es sich wirklich um ein Thema handelt, wo Grenzfragen militärischer, aber eben auch ziviler Sicherheit angesprochen werden, ist das vielleicht ein Forum, in dem man also auch über solche Fragen diskutieren kann."[87]

„Es geht eigentlich nur um militärische Bedrohungen. Etwa wenn man sich anguckt, was da als die drei wesentlichen Bedrohungen für die Alliierten in den nächsten zehn Jahren genannt wird, dann ist es erstens ein Raketenangriff durch den Iran, zweitens Angriffe internationaler terroristischer Gruppen und drittens ein Cyber-Angriff mit unterschiedlicher Intensität."[88]

„Wenn wir jetzt über den Aufbau von zivilen Fähigkeiten sprechen und dazu noch Cyber-Defense als integrierte Struktur mit aufgebaut werden soll: Passt das überhaupt in die Reform-Überlegungen der NATO-Größe oder gibt es dann tatsächlich eine komplett neue Schüttelung, Reduzierung des militärischen, Aufbau des Zivilen?"[89]

„Es ist völlig richtig, dass die NATO Bedrohungen definiert. Aber wir dürfen – und das sollte die NATO auch nicht tun – nicht den Fehler machen, dass zwischen der Feststellung einer Bedrohung und Festlegung, wer denn ggfs. für die Abwendung dieser Bedrohung zuständig ist, einen zu engen Kontext machen. Ich will das aus meiner Sicht - da mache ich aus meiner Meinung überhaupt keinen Hehl - am Beispiel Cyber erläutern. Völlig zu Recht und gerade nach den neus-

[85] Ebenda, S. 29.

[86] Prof. Dr. Dr. Hans J. Gießmann, Berghof Forschungszentrum für konstruktive Konfliktbearbeitung, ebenda, S. 13.

[87] Ebenda, S. 31.

[88] Prof. Dr. Michael Brzoska, Institut für Friedensforschung und Sicherheitspolitik, ebenda, S. 15.

[89] Roderich Kiesewetter, MdB, ebenda, S. 17.

ten Dingen, die die ganze Welt alarmiert hat, ist eine Cyber-Attacke eine Bedrohung. Und völlig zu Recht sage ich auch, dass die Bundeswehr dafür da ist, ihre eigene militärische Infrastruktur zu schützen. Aber ich kann überhaupt nicht erkennen, dass das Instrument, was wir im Rahmen der NATO haben - die NATO ist ein politisches Bündnis mit militärischen Instrumenten -, dass wir dieses Instrument Bundeswehr haben, automatisch verwenden sollten, um die Abwehr möglicher Cyber-Attacken zu nehmen. Das ist für mich überhaupt nicht gegeben, dieser Kontext. Ich würde sogar, ohne dass ich mich darin vertieft habe, davor warnen, das so zu tun. Ich würde im Zweifel sagen: Angenommen, es gäbe eine Cyber-Attacke ganz gezielt auf die deutsche Automobil-Industrie, damit die Bänder still stehen, dann würde ich nicht sehen, dass BMW, Daimler Benz, Audi und Porsche, wie sie alle heißen, dann sagen, das soll jetzt die Bundeswehr lösen. [...] Ich sage sehr, sehr deutlich, dass ich von einer Verbindung zwischen Cyber Attac und einem Automatismus von Art. 5 überhaupt nichts halte. Was wir bisher von möglichen Cyber Attacs sehen, ist so, dass sie sehr komplex sind, dass sie zum Teil kaum aufspürbar sind, dass da ein Server steht in Honolulu und einer in Afrika, ein dritter steht in Australien. Der Software-Mensch sitzt wo auch immer. Und wir wissen auch gar nicht genau, wo das Ziel ist. Und jetzt daraus eine Art. 5-Operation abzuleiten, halte ich nahezu für abenteuerlich. Da möchte ich aber sagen, das ist meine persönliche Meinung und ich kann nur hoffen, dass sich diese meine Meinung im NATO-Konzept auch wiederspiegelt.“[90]

„Und dann als dritter Bereich der sogenannte Cyber War, wo ja gesagt wird, das ist die zentrale neue konventionelle Bedrohung […] Es steht ja in seinem Beitrag auch. Da ist die Frage, soll da Art. 5 wirksam werden? Was muss man sich darunter vorstellen? Wie hat man sich das vorzustellen? Und ganz zentral natürlich die Frage der Vermischung von ziviler und militärischer Infrastruktur, wenn Sie sich überlegen, welch zentrale Bedeutung die elektronische Kommunikation für Wirtschaft und Gesellschaft in unserem Land hat. Bei uns ist für den Schutz dieser Infrastruktur bisher der Innenminister zuständig. Dann weiß man, was das bedeutet, wenn hier eine Eingrenzung des Militärischen in Bezug auch auf polizeiliche Aufgaben stattfindet. Das ist eine neue Qualität, die unser Grundverständnis von Gewaltenteilung in einer modernen Demokratie in den Grundfesten, wirklich in den Grundfesten, in Frage stellt. Auch hier meine Frage: Es gibt ja schon Praxis - seit Mai nach meiner Kenntnis -, ein Strategisches Cyber-Oberkommando der USA in Ford Meade, die ja gewissermaßen die Vorgaben machen, in dem man überlegt. Die Bundeswehr hat ja im letzten Jahr immerhin eine entsprechende Abteilunge eingerichtet im Kommando Strategische Aufklärung. Also auch vor diesem Hintergrund, wie verläuft da die Debatte? […] Wie definiert man da den Verteidigungsfall und wer ist da eigentlich zuständig? Und wir alle haben ja auch die Diskussion über Stuxnet verfolgt, wo man sich ja fragt, wie offensiv der Cyber War sozusagen durchaus von Seiten des Westens eigentlich schon stattfindet. Wir glauben doch immer, wir könnten darüber diskutieren. Wird er überhaupt Bestandteil der Strategie und wie kontrollieren wir ihn? Vielleicht findet er ja schon statt, das ist ja eine Vermutung, die aufkommt. Also vor diesem Hintergrund, wie sehen Sie das? Und vor allen Dingen wäre das ja eine Frage der präventiven Rüstungskontrolle, wie im Bereich der BNC-Waffen auch. Das ist ein so zentraler Bereich unserer Gesellschaft und das muss eigentlich militärisch eine no-go-area sein. Da müsste man ja eigentlich über Konventionen nachdenken, wie wir das im Bereich der Chemie- und der biologischen Waffen auch haben. Und wir müssten es thematisieren als Be-

[90] Dr. Rainer Stinner, MdB, ebenda, S. 19.

standteil präventiver Rüstungskontrolle. Mir ist aufgefallen, dass niemand von Ihnen das auch nur in diesem Zusammenhang thematisiert hat. Da würde ich die Frage stellen, warum eigentlich nicht? Danke.“[91]

„Ich möchte meinen Fokus auch ganz kurz auf den Aspekt des Cyber-Attac richten. Wir alle wissen, Art. 5 ist sicher Hardcore des Strategischen Konzepts der NATO und wird es auch in Zukunft bleiben. Bisher war es ja so, dass, wenn fundamentale Sicherheitsinteressen z.B. durch militärische Angriffe berührt sind, dass dann die Solidaritätsverpflichtung des Art. 5 griff. Jetzt wissen wir, die Zeiten ändern sich, auch die Bedrohungen und Risiken ändern sich und immer mehr kommt in den Fokus: Angriffe auf Energie-Infrastruktur, Angriffe auf Transit-Areas, aber auch Angriffe im Wege von Cyber Attac. Nun hat ja Herr Stinner Angriffe auf die Automobil-Industrie angesprochen. Ich kann mir aber auch vorstellen, dass es im Sinne von Cyber Attac Angriffe auf essentielle Institutionen und Einrichtungen eines Staates gibt. Ich denke an den Bereich Elektrizität, ich denke an den Bereich Wasser, die die Sicherheitsinteressen eines Landes fundamental berühren. Und deswegen meine Frage: Ist es denkbar, dass wir über Art. 4 – den haben wir heute noch gar nicht genannt, also Auslösung eines Konsultationsmechanismus in einem solchen Fall – dann zu Art. 5 kommen, wenn wirklich auf diesem Wege fundamentale Sicherheitsinteressen eines Bündnispartners berührt sind? Vielen Dank.“[92]

7.2. Debatte

Der Deutsche Bundestag hat am 11. November 2010 eine Debatte zum neuen Strategischen Konzept der NATO geführt. Im nachfolgenden werden hieraus wesentliche Argumente zum Thema der Cyber-Sicherheit geordnet nach Mitgliedern der Fraktionen aufgeführt.[93] Hierbei wurde darauf geachtet, Positionen vorzugsweise nicht zu wiederholen, sondern die Breite der Argumente vorrangig aufzuzeigen.

CDU/CSU-Fraktion:

„Cyberattacken und mögliche Angriffe auf Handelsrouten und unsere Energieversorgung sind neue Dimensionen der konkreten Bedrohungen für unser Land.“[94]

„Wir stehen heute vor ganz anderen Herausforderungen. Deshalb finde ich es richtig, dass sich die NATO um die Frage der Cyberattacken bemüht, selbst wenn das nur der Beginn einer Diskussion sein kann. Hier gibt es viele Fragen zu den Fähigkeiten der NATO. Die Frage ist auch

[91] Dr. Frithjof Schmidt, MdB, ebenda, S. 22.

[92] Dr. Karl A. Lamers (Heidelberg), MdB, ebenda, S. 23.

[93] Deutscher Bundestag, Plenarprotokoll 17/71, 11. November 2010, S. 7599 ff., URL: http://dipbt.bundestag.de/dip21/btp/17/17071.pdf [10.03.2011].

[94] Dr. Andreas Schockenhoff, ebenda, S. 7602 (B).

[…] Wie geht man im Fall des Falles damit um? Wir stellen uns diesen Fragen in der Diskussion; wir wollen sie weiter in den Blick nehmen.“[95]

„Bei neuen Bedrohungen denke ich zum Beispiel an Cyberangriffe. Millionen Angriffe finden täglich statt: auf Staaten, Sicherungssysteme von Industrieanlagen, Banken und Pipelines. Das ist eine Gefahr, die uns existenziell bedrohen kann. Cybersicherheit muss stärker als bisher auch in das Blickfeld der NATO rücken. Da ist es nicht geeignet, hier Witzchen wie ‚Google bombardieren‘ zu machen. Vielmehr sollte auch für Sie gelten, dass das ein wichtiges Thema ist, das in einer politisch-militärischen Institution wie der NATO seriös erörtert wird.“[96]

„Sie müssten erklären, warum die NATO die Augen vor der Bedrohung unserer Computersysteme verschließen soll, von denen nicht nur die Krankenhäuser, der Straßenverkehr und die Elektrizitätsversorgung abhängen.“[97]

„Es kennzeichnet die neuen Bedrohungslagen, dass sie vielfach nicht militärischer Natur sind, von nichtstaatlichen Akteuren ausgehen und deswegen auch nicht allein mit militärischen Mitteln bewältigt werden können. Dennoch sind diese neuen Bedrohungen – von Angriffen auf Computernetze über Proliferation von Massenvernichtungswaffen bis zu Terrornetzwerken – Teil einer weit gefassten Definition des Sicherheitsbegriffs. Von daher ist es notwendig, dass die NATO sie in ihr neues Strategisches Konzept aufnimmt.“[98]

SPD-Fraktion:

„Ich stimme mit dem überein, was hier von einigen Kollegen zu Cyber gesagt worden ist; dies kann nicht nach Art. 5 erfolgen.“[99]

FDP-Fraktion:

„Es gibt einen weiteren neuen Aspekt in dem NATO Konzept, und das ist Cyberwar; darauf ist hingewiesen worden. Ich möchte Sie aber bitten, Herr Außenminister, in der nächsten Woche, vor Verabschiedung des Konzepts, darauf hinzuarbeiten, dass wir jedenfalls nicht einen Automatismus zwischen Cyberbedrohung und Art. 5 NATO-Vertrag bekommen. Ich sehe das sehr kritisch. – Ich sage das ja so. Liebe Kollegin, ich sage deutlich, wie ich es empfinde. Ich sehe es sehr kritisch, dass wir einen Automatismus zwischen Cyberattacken und Art. 5 herstellen sollen. Hier müssen wir sehr genau hinschauen. Ich möchte die Verbindung so unverblümt möglichst nicht in dem Konzept haben.“[100]

---

[95] Philipp Mißfelder, ebenda, S. 7611 (D).

[96] Dr. Karl A. Lamers (Heidelberg), ebenda, S. 7614 (A).

[97] Ruprecht Polenz, ebenda, S. 7618 (D).

[98] Thomas Silberhorn, ebenda, S. 7619 (B).

[99] Uta Zapf, ebenda, S. 7610 (C).

[100] Dr. Rainer Stinner, ebenda, S. 7608 (D).

Fraktion BÜNDNIS 90/DIE GRÜNEN:

„Jetzt stellen wir fest, dass eine Suche nach neuen Aufgaben innerhalb der NATO stattfindet. Es ist die Rede vom Cyberwar. Ja, der Cyberwar ist eine Bedrohung. Nur, ist diese Bedrohung mit den Instrumenten der NATO zu lösen? Was wollen Sie denn tun? Google bombardieren? Das kann doch keine ernsthafte Alternative sein.“[101]

Fraktion DIE LINKE:

Keine Stellungnahme.

8. 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).“[102] Und zum anderen auch durch das Bekenntnis der Bundeskanzlerin, Dr. Angela Merkel, dass „die Bedrohung nicht weniger gefährlich als klassische militärische Angriffe (sei).“[103] 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 ebenso wie die Kommission der Europäischen Union 2009. 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

[101] Jürgen Trittin, ebenda, S. 7602 (D).

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

[103] “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 [14.04.2011].

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.[104]
- 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 Herkulesaufgabe 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.“[105]

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

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

[105] „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 [14.04.2011].

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]