Alexander Niedermeier

Nicht(s) auf dem Radar: Cyberkrieg als komplexe Herausforderung für die hochgradig vernetzte Gesellschaft

»The next wars will be fought not just on battlefields but also in the world's computers and communications systems. The combatants will often be familiar powers – like China, France, and Russia – but there will be others, including underestimated powers, like India; presumed allies, like Israel; and countries that hardly seem to have any military capability at all, like the Philippines.«[1] *(Bruce Berkowitz, 2003)*
»It is now clear that this cyber threat is one of the most serious economic and national security challenges we face as a nation. It's also clear that we're not as prepared as we should be, as a government or as a country.«[2] *(Barack Obama, 2009)*
»Unbemerkt haben die Streitkräfte zahlreicher Länder auf einem neuen Schlachtfeld Aufstellung genommen. Weil man sie nicht sieht, haben die Parlamente und die Bevölkerung die Truppenbewegungen nicht bemerkt. Bisher wissen nur wenige wozu Cyberkrieger in der Lage sind. Weil die meisten große Militärmächte Handelspartner sind, können sich die Beobachter nicht vorstellen, dass die Beziehungen in Feindseligkeiten umschlagen.«[3] *(Richard A. Clarke / Robert K. Knake, 2011)*

1. Cyberkrieg: Neue Herausforderung für eine hochgradig vernetzte Gesellschaft

Stuxnet, *Conficker*, *Orchard*, *Moonlight Maze*, *Code Red* oder *Buckshot Yankee*: Die wenigsten Deutschen außerhalb der Cyber-Community dürften auf Anhieb wissen, was mit diesen ungewöhnlichen Namen gemeint ist. Und dennoch handelt es sich hierbei um getestete oder bereits tatsächlich eingetretene Szenarien moderner Kriegführung, welche nicht nur seit geraumer Zeit dazu beitragen, das militärische Schlachtfeld nachhaltig zu verändern, sondern auch potenziell geeignet sind, bereits auf sehr absehbare Zeit das globale Mächtegleichgewicht grundlegend zum Nachteil der bislang dominierenden Akteure zu verschieben. Zugleich stellen die Strukturen und Prozesse, welche mit den eingangs angeführten Namen verbunden sind, auch eine vielschichtige Bedrohung für unser derzeitiges freiheitlich-liberales Modell demokratischer Rechtsstaatlichkeit und letztlich

1 Bruce Berkowitz, *The New Face of War. How War Will Be Fought in the 21st Century*, New York 2003, S. 1.
2 Barack Obama, Remarks by the President on securing our national cyber infrastructure, http://mcaf.ee/roqjh (Stand 8.12.2011).
3 Richard A. Clarke / Robert K. Knake, *World Wide War. Angriff aus dem Internet*, München 2011, S. 317.

der heute vorherrschenden Lebensweise per se dar. Angesichts jener Diskrepanz aus umfassender Bedrohungslage einerseits und hohen Bewusstseinsdefiziten andererseits möchte sich dieser Beitrag mit den Fragen auseinandersetzen, was das Wesen des Cyberkrieges ist, wie es zur bestehenden Verletzlichkeit kam und welche sicherheitsrelevanten Konsequenzen sich hieraus für die moderne hochgradig vernetzte Gesellschaft ergeben. Hierbei soll kritisch aufgezeigt werden, wie die Herausforderungen von verschiedenen Akteuren wahrgenommen werden und welche Reaktionen bislang erfolgt sind. Nicht zuletzt sollen Wege skizziert werden, die darauf weisen welcher Umgang in den Bereichen Militär, Wirtschaft, Recht und Gesellschaft als geeignet erscheint, um letztlich das bestehende Gesellschaftsmodell bestmöglich zu wahren. Da Cyberkrieg im vorliegenden Beitrag dem zwischenstaatlichen Krieg zugerechnet wird, werden Cyberterrorismus, Cyberkriminalität etc., obgleich zum Teil durchaus verwoben, nicht behandelt. Die zentralen Akteure sind die sogenannten Advanced Persistent Threats (APTs), unter denen von Nationalstaaten kontrollierte (Militär, Sicherheitsbehörden etc.) oder beauftragte Gruppen (kommerzielle Unternehmen, Cybersöldner etc.) verstanden werden.[4]

1.1 Frei, demokratisch, ignorant: Die unvorbereitete Gesellschaft und ihre Gefährdung

Betrachtet man die eingangs angedeuteten vielschichtigen Herausforderungen, so erscheinen diese gar nicht unbedingt als etwas fundamental Neues; auch der (vorerst?) zu Ende gegangene Kalte Krieg war geprägt von einer stets latenten Bedrohung der jeweiligen politischen Blöcke und der durch sie repräsentierten ökonomischen und sozialen Ordnungsmodelle. Die Generationen der Kalten Krieger, egal ob Teil der Eliten oder einfache/r Bürger/in, waren sich dieser ubiquitären Gefährdung jedoch die letzten Jahrzehnte hindurch stets deutlich bewusst. Man kannte die Wirkungen eines nuklear geführten Krieges, es existierten empirische Beispiele dafür, wie das Handeln der Supermächte auf die politischen, wirtschaftlichen und gesellschaftlichen Systeme dritter Staaten wirken konnte. Dergleichen trifft heute nicht mehr zu. Zwar haben sich neue Bedrohungsperzeptionen und Feindbilder etabliert, wie etwa der gewaltbereite politische Islam oder ein nuklear aufgerüsteter Iran, beides durchaus Szenarien, welche es bei der nationalen Sicherheitsplanung ernst zu nehmen gilt, jedoch hat sich im Laufe der letzten beiden Dekaden eine weitere Form möglicher Kriegführung entwickelt, welche gleichermaßen von den verantwortlichen Eliten wie auch insbesondere der breiten Öffentlichkeit gerade hierzulande kaum beziehungsweise nur ganz allmählich wahrgenommen wird. Darauf, dass es sich tatsächlich um mehr handelt als um weit hergeholte Ideen einer hochspezialisierten Community, lässt sich nicht nur daran ablesen, wie ernst seit jüngster

4 Vgl. Jason Andress / Steve Winterfield, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Waltham 2011, S. 29ff.

Zeit immer mehr ausländische Regierungen das Thema nehmen[5], sondern auch, dass in wachsender Zahl und Gravität Vorfälle auftreten, welche sich der derzeit konzeptionell immer weiter ausgestaltenden Domäne der Cyberkriegführung zurechnen lassen.[6] Gleichwohl erobert sich das Thema den ihm gebührenden Platz im deutschen öffentlichen Diskurs viel zu schleppend. Lediglich vereinzelt lassen sich Beiträge in den Breitenmedien Zeitung, Fernsehen und Rundfunk finden. Und auch die wissenschaftlichen Publikationen der deutschen Scientific Community halten sich ebenso wie Übersetzungen einschlägiger ausländischer Werke angesichts der enormen praktischen Wirkungsmächtigkeit des Themas viel zu sehr in Grenzen. So liegen neben einer Handvoll Studien und Aufsätzen zum Thema[7] derzeit nur sehr wenige entsprechende Monografien[8] vor. Obgleich die Bedrohung durch Cyberkriege etwa auch im Bewusstsein der amerikanischen Öffentlichkeit wie auch der Privatwirtschaft ebenfalls viel zu wenig präsent ist und auch den vergangenen US-Regierungen vorgeworfen werden kann, aus verschiedenen Motivationen heraus, das Problem unterschätzt oder vernachlässigt zu haben[9], wenngleich freilich in einem deutlich geringeren Maße als hier, so gilt es doch zu konstatieren, dass dort eine Vielzahl relevanter Veröffentlichungen erschienen ist, teils durch Think Tanks, teils durch militärische oder öffentliche Institutionen und teils aus den Reihen der wissenschaftlichen Sicherheitsstudien. Allerdings ist dabei auffällig, dass der Cyberkrieg bislang keinen Eingang in die generelle Debatte um die sogenannten neuen Kriege gefunden hat, obwohl ja bei diesen gerade der auch für den Cyberkrieg so entscheidende Aspekt der Asymmetrie zentral ist.[10] Angesichts jenes weit verbreiteten Bewusstseins-

5 Vgl. etwa Sandro Gaycken, *Cyberwar. Das Internet als Kriegsschauplatz*, München 2011, S. 69-74, sowie Nick Hopkins, »Stuxnet attack forced Britain to rethink the cyber war«, http://mcaf.ee/ir4hc (Stand 3.11.2011), sowie Artikel» Basij lawyers to confront ‚enemy' in cyber warfare«, http://mcaf.ee/s3xvd (Stand 8.12.2011.).

6 Vgl. etwa Gaycken, Cyberwar, aaO. (FN 5), S. 169-180, sowie Clarke / Knake, *World Wide War,* aaO (FN 3), S. 29-57.

7 Vgl. etwa Friedrich Wilhelm Kriesel / David Kriesel, »Cyberwar – relevant für Sicherheit und Gesellschaft? Eine Problemanalyse« in: *ZfAS* Nr. 4 (2011), S. 205-216, sowie Olivier Minkwitz, *Ohne Hemmungen in den Krieg? Cyberwar und die Folgen*. HSFK-Report 10/2003, sowie Jörg Wollscheid, Postmoderner Krieg. Die Verflechtungen von Krieg und Medientechnik und die Auswirkungen auf die Außen- und Sicherheitspolitik der Staatenwelt zu Beginn des 21. Jahrhunderts, Trier 2004, S. 118-145, sowie Frank Sauer, »In *Byte*gewittern? Fragwürdige Konzepte von Krieg und Terror im Cyberspace« in: Jan Helmig, / Niklas Schörning, (Hg.), *Die Transformation der Streitkräfte im 21. Jahrhundert. Militärische und politische Dimensionen der aktuellen »Revolution in Military Affairs«*, Frankfurt a.M./New York 2008, S. 103-123.

8 Hierbei handelt es sich v.a. um Gaycken, Cyberwar, aaO. (FN 5), und Clarke / Knake, aaO. (FN 3), und Günther K. Weiße, *Informationskrieg und Cyberwar. Die unbekannte Gefahr*, Stuttgart 2007 und Arne Schönbohm, *Deutschlands Sicherheit. Cybercrime und Cyberwar*, Münster 2011, und Tillmann Schulze, *Bedingt abwehrbereit. Schutz kritischer Informationslnfrastrukturen in Deutschland und den USA*, Wiesbaden 2006.

9 Vgl. etwa Clarke / Knake, World Wide War, aaO. (FN 3), S. 181ff.

10 Vgl. etwa Herfried Münkler, *Die neuen Kriege*, Hamburg 2002, sowie Michael Brzoska, »'New Wars' Discourse in Germany« in *Journal of Peace Research* 41, Nr. 1 (2004), S. 107-117, sowie Malesevic, Sinisa, »The Sociology of New Wars? Assessing the Causes and Objectives of Contemporary Violent Affairs« in: *International Political Sociology* Nr. 2 (2008), S. 97-112, sowie

defizits ziehen Clarke und Knake auch bei ihrem auf die USA gerichteten Blick eine Parallele zur Situation vor dem Ausbruch des Ersten Weltkrieges, wie sie von Barbara Tuchman in ihrem berühmten Werk *Der Stolze Turm* beschrieben wurde. Damals wie heute sieht es so aus, als lasse sich eine Gesellschaft vorfinden, »die ähnlich abgelenkt ist und nicht wahrnimmt, dass das Militär in zahlreichen Ländern enorme Streitkräfte aufbaut, ohne die furchtbaren Konsequenzen zu bedenken. Ein Funken genügte, um das Pulverfass explodieren zu lassen«[11].

In der Tat sind es andere Themen, welche derzeit die hiesigen Diskurse um Internet einerseits und Militär und nationale Sicherheit andererseits bestimmen. Das Problematische dabei ist vor allem, dass die beiden Diskurse, obwohl ihre Gegenstände aufs Engste verzahnt sind, keine diskursive Deckungsmenge aufweisen, soll heißen gleichsam berührungsfrei nebeneinander existieren. So ist der Diskurs um das Internet bestimmt von Fragen des persönlichen Datenschutzes, der möglichen Überwachung durch staatliche Stellen, der Einflussmöglichkeiten der privaten Internetwirtschaft oder kommerziellen Internetbetrugs; der Diskurs um Militär und nationale Sicherheit indes dreht sich um Aspekte wie Terrorismus, Wehrpflicht, Standortschließungen oder Auslandseinsätze der Bundeswehr, wobei es hierbei primär um normative oder demokratietheoretische Fragen wie etwa die Notwendigkeit der Einbindung des Parlaments in die Entscheidungen im Bereich der klassischen Regierungsdomäne Außen- und Sicherheitspolitik geht. Aber auch in den zuständigen Ressorts der gegenwärtigen Bundesregierung ist unklar, wie der Herausforderung Cyberkrieg effektiv begegnet werden soll. Diesbezüglich agiere man dort nicht selten »im Nebel«, entsprechende Planungen hierzu steckten derzeit trotz anderweitiger offizieller Verlautbarungen noch weitgehend »in den Kinderschuhen«.[12] Und auch wenn Deutschland damit angefangen hat, in administrationsorganisatorischer und militärischer Hinsicht zu reagieren und etwa eigene militärische Cyberkräfte aufzustellen[13], so sind die Maßnahmen und Kapazitäten im Vergleich mit Staaten wie den

Edward Newman, »The 'New Wars' Debate: A Historical Perspective is needed« in: *Security Dialogue* 35, Nr. 2 (2004), S. 174-189.

11 Clarke / Knake, World Wide War, aaO. (FN 3), S. 317; vgl. zudem Barbara W. Tuchman, *Der stolze Turm. Ein Portrait der Welt vor dem Ersten Weltkrieg. 1890-1914*, München/Zürich, 1969.

12 Informelle Gespräche mit mehreren Verantwortlichen im Umfeld zuständiger Stellen im November 2011. Die Gesprächspartner baten darum, nicht genannt zu werden. Vgl. zudem Artikel: Verteidigungsminister warnt vor »Cyber War«, http://www.focus.de/politik/weitere-meldungen/guttenberg-verteidigungsminister-warnt-vor-cyber-war_aid_571532.html (Stand 8.12.2011).

13 Vgl. etwa Klaus-Dieter Fritsche, *Cyber-Sicherheit. Die Sicherheitsstrategie der Bundesregierung*, Berlin 2011, sowie Schönbohm, Deutschlands Sicherheit, aaO. (FN 8), S. 59-85, sowie Armin Käfer, »Deutschland wappnet sich«, http://mcaf.ee/50g8r (Stand 6.12.2011), sowie Achim Killer, »Wie die Bundeswehr den ‚Cyberwar' gewinnen will«, http://mcaf.ee/76lga (Stand 8.12.2011), sowie Artikel: »Bundeswehr baut geheime Cyberwar-Truppe auf«, http://mcaf.ee/go0pl (Stand 8.12.2011), sowie Deutscher Bundestag, Drucksache 17/7118 vom 4.10.2011.

USA, China oder Nordkorea in jeder Hinsicht unzureichend.[14] Dieser Umstand wird nicht nur an den zersplitterten Zuständigkeiten in der BRD deutlich[15], sondern auch an der aktuellen Politik der Bundesregierung, welche nicht zuletzt ihren Niederschlag in deren Sicherheitsstrategie findet. So sind etwa die ausgewiesenen Investitionen (inklusive Betriebskosten) für relevante Cybermaßnahmen in Höhe von 360 Millionen Euro[16] viel zu gering wenn man sie mit dem Budget der *Comprehensive National Cybersecurity Initiative* des Nationalen Sicherheitsrates der US-Regierung vergleicht, deren Etat bei 18 Milliarden US-Dollar liegt.[17] Ferner werden nur Hilfestellungen und Handlungsempfehlungen für private Nutzer gegeben, jedoch keine klaren gesetzlichen Vorgaben etwa für privatwirtschaftliche Betreiber kritischer Infrastrukturen.[18] Auf internationaler Ebene gibt es zwar eine Abstimmung mit verbündeten Staaten, ebenso kommt es zu Teilnahmen an internationalen Übungen[19], jedoch blieb eine erkennbare Doktrinentwicklung bislang ebenso aus wie etwa Vorschläge zur Regelung der Cyberkriegsherausforderungen auf der Ebene des internationalen Rechts; insbesondere eine Positionierung zwischen den verschiedenen Vorschlägen etwa Russlands und der USA blieb die Bundesregierung, aber ebenso der öffentliche Diskurs, bislang schuldig. Fast erscheint es daher so, als befinde man sich in einer Situation, welche jener vergleichbar ist, die sich zu Mitte des 20. Jahrhunderts stellte, als zwar Atom- und Wasserstoffbomben real existierten, aber der Umgang damit gleichermaßen unklar wie umstritten war. Auch damals fehlten noch viele Erfahrungswerte, auch damals musste eine Doktrin erst entwickelt werden. Heute allerdings wird das Problem durch die oben geschilderte Tuchman-Analogie verkompliziert und negativ beeinflusst. Zudem können der militärische und der zivile Bereich de facto nicht mehr klar getrennt werden. Eine Suche nach dem geeigneten Umgang auf politischer, militärischer, privatwirtschaftlicher und (zivil-)gesellschaftlicher Ebene erfordert eine signifikante Steigerung des Bewusstseins für das Problem

14 Vgl. etwa Andress, / Winterfield, *Cyber Warfare*, aaO. (FN 4), S. 69-74, sowie Gaycken, Cyberwar, aaO. (FN 3), S. 180-190, sowie Clarke / Knake, World Wide War, aaO. (FN 3), S. 43-50, sowie Babette M. Marvel (Hg.), *China's Cyberwarfare Capability*, New York 2010, sowie Vinod Anand, »Chinese Concepts and Capabilities of Information Warfare« in: *Strategic Analysis* 30, Nr. 4 (2006), John J. Tkacik, Jr., »Trojan Dragons: China's Cyber Threat«, in: *Backgrounder* Nr. 2106 (2008), S. 1-12, sowie John Oakley, Cyber Warfare: China's Strategy to Dominate in Cyber Space, M.A. Thesis, Fort Leavenworth 2011, sowie Bryan Krekel, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, McLean 2009, sowie Mok Yoong Jae, »North Korea's Powerful Cyber Warfare Capabilities« , http://mcaf.ee/768nm (Stand 8.12.2011), sowie James A. Lewis, »Speak Loudly and Carry a Small Stick: The North Korean Cyber Menace«, http://mcaf.ee/myucr (Stand 8.12.2011.).

15 So ist das Bundesverteidigungsministerium für offensive Cyberkriegführung zuständig und das Bundesinnenministerium (genau: das ihm untergeordnete Bundesamt für Sicherheit in der Informationstechnik) für den defensive Cyberewarfare. Vgl. hierzu auch Kriesel / Kriesel, *Cyberwar,* aaO. (FN 7), S. 211.

16 Vgl. Fritsche, Cyber-Sicherheit, aaO. (FN 13), S. 4.

17 Vgl. Jason Andress, / Steve Winterfeld, aaO. (FN 4), S. 240.

18 Zur Definition kritischer Infrastrukturen vgl. etwa John Moteff / Paul Parfomak, *Critical Infrastructure and Key Assets*: *Definition and Identification*, Washington 2004.

19 Vgl. etwa Fritsche, Cyber-Sicherheit, aaO. (FN 13), S. 4.

ebenso wie die Erhöhung des Wissens um die aktuellen Entwicklungen. Doch »[s]tatt die globalen Veränderungstrends aktiv zu gestalten, fährt die Politik im Energiesparmodus. Aber auch viele Bürger huldigen dem Status quo«[20], wie Wolfgang Ischinger, langjähriger Diplomat und zuletzt Vorsitzender der Münchener Sicherheitskonferenz, feststellt. In diesem Zusammenhang verweist er darauf, dass nicht zuletzt der Cyber-Krieg, der für »dramatische Wandlungsprozesse mit gewaltigen Folgen für globale Sicherheit und Stabilität«[21] stehe, hierzulande ignoriert werde: »[D]ie Deutschen hätten es lieber, wenn sich nichts verändern würde, weil es schlimm genug ist, so wie es ist – und weil weitere Veränderungen nichts Gutes verheißen«.[22] Dabei ist gerade dieses Rückzugsphänomen angesichts der zunehmenden Vernetzung von Zivilgesellschaft, Wirtschaft, wobei Industrie, Handel und Finanzwesen gleichermaßen gemeint sind, Militär und Politik, fatal, nicht zuletzt weil jedes Sicherheitsnetz letztlich nur so stark sein kann wie sein schwächstes Glied. Und angesichts der Entwicklungen im Bereich des Cyberkrieges zeigt sich, dass der zunehmende Grad der Vernetzung auf verschiedensten Ebenen und in den unterschiedlichsten Bereichen dazu führt, dass es eine Vielzahl von Gliedern gibt, von welchen *jedes für sich* potenziell geeignet ist, die nationale Sicherheit auf *allen* Ebene zu gefährden.[23] Die größte Gefahr, der sich die hochtechnisierten und hochgradig und in weiterhin zunehmendem Maße vernetzten westlichen Industrie- beziehungsweise Post-Industriegesellschaften ausgesetzt sehen, ist, dass sie just jene Faktoren verletzlich machen und ihre bisherige Dominanz gefährden, welche diese erst ermöglicht und lange Zeit gewährleistet haben.

1.2 Wie aus Stärke Schwäche wurde: Zur Entwicklung des Cyberkrieges und den Folgen für die hochgradig vernetzte Gesellschaft

Dies gilt zunächst und in besonderem Maße für den militärischen Sektor, wo Vernetzung und Interoperabilität zu den zentralen Größen geworden sind. Berkowitz schreibt in seiner Studie über die Kriegführung im 21. Jahrhundert, dass »Information technology is so important in war today that it overwhelms everything else«[24]. Hierzu passt die Aussage, welche Oberst Kilroy vom Virginia Military Institute im Rahmen eines Gastvortrages an der Duke University im Herbst 2009 äußerte, der zufolge heute nicht mehr der Kommandant sondern der Systemadministrator die de facto wichtigste Person in Stützpunkten etc. sei und folgerichtig auch am besten bewacht und im Notfall auch als

20 Wolfgang Ischinger, »*Deutschland bitte aufwachen*«, http://mcaf.ee/ar2g6 (Stand 8.12.2011).
21 Ebd.
22 Ebd.
23 Vgl. zu den verschiedenen Ebenen und Dimensionen der nationalen Sicherheit das Modell der Hierarchiepyramide des komplexen nationalen Sicherheitsinteresses, das sich findet bei Alexander Niedermeier, »Was kann der Interpretative Realismus leisten? Zwischenstaatliche Kooperation und die künftige Gestalt der EU als Herausforderung für die Theoriebildung« in: Eckhard Jesse, / Gerd Strohmeier, / Roland Sturm (Hg.), *Europas Politik vor neuen Herausforderungen*, Opladen/Farmington Hills 2011, S. 365-385, insbes. S. 380ff.
24 Berkowitz, The New Face of War, aaO. (FN 1), S. 3.

erstes in Sicherheit gebracht werde.[25] Die Grundlagen dieser Entwicklung, welche zunächst eine nie gekannte Überlegenheit und nun eine exorbitante Verwundbarkeit mit sich gebracht hat, wurde mit dem Übergang vom Konzept der plattformzentrierten (*Platform-Centric Warfare*, PCW) zur netzwerkzentrierten Kriegführung (*Network-Centric Warfare*, NCW) eingeleitet.[26] Hierbei handelt es sich um eine militärische Theorie, welche seit den 1990er Jahren zusehends durch die praktischen Entwicklungen zu einer Doktrin des informationsbasierten kinetischen Krieges entwickelt wurde. Eckpfeiler hierbei waren ein verbesserter Austausch an Informationen durch die eigenen Streitkräfte um zu Echtzeitdarstellungen auf strategischer wie taktischer Ebene zu gelangen. Das so gesteigerte situative Bewusstsein sollte zu neuen Organisationsstrukturen und Verfahren und so zu einem verbesserten Zusammenspiel der Einsatzkräfte sowie zu zunehmender Selbstsynchronisierung führen und so die Effizienz militärischer Missionen nachhaltig erhöhen. Konkrete Ausgestaltung erfuhr der Ansatz 1996 durch das sogenannte *System-der-Systeme-Konzept* von Admiral William Owens, welches den Einsatz netzwerkbasierter Kommando- und Kontrollsysteme, netzwerkgesteuerter Präzisionswaffen etc. vorsah. Zeitgleich wurde von den Vereinten Stabschefs das Konzept der *Joint Vision 2010* vorgestellt, welches darauf ausging, mit Hilfe der neuen Möglichkeiten der Informationstechnologien eine Dominanz über alle militärisch relevanten Bereiche zu erlangen (*Full Spectrum Dominance*). Eine theoretische wie konzeptionelle Verfestigung erhielt das Konzept des NCW durch Vizeadmiral Arthur K. Cebrowski, wobei zahlreiche Konzepte des zivilen Sektors auf militärische Strukturen übertragen wurden.[27] Durch die Aufgliederung in die materielle, die informationelle und die kognitive Ebene schließlich erfolgte eine weitere analytisch-konzeptionelle Verfeinerung des NCW, welche Aspekte der kognitiven Psychologie bezüglich der Wahrnehmung und Interpretation von Systeminformationen aufnahm.[28] Ausgehend von einer Kritik an der sich entwickelnden realen Form des NCW, welche zu komplex für die bisherige Militärorganisation auf allen Ebenen sei, wurde versucht, einen noch dezentralisierten, und dabei noch mehr auf grundlegende Vernetzung setzenden Ansatz zu entwickeln, für den die Idee des sogenannten *Global Information Grid* eine Ausgangsbasis darstellen soll-

25 Der Gastvortrag fand im Rahmen einer Lehrveranstaltung an der Duke University statt, welche der Verfasser des Artikels im Rahmen im Herbssemester 2009 zum Thema *European Perspectives on National Security. A Micro and Macro Level Approach of Analysing National Security* gemeinsam mit Constantin Schlachetzki abhielt.

26 Zu NCW vgl. etwa David S. Alberts / John J. Garstka / Frederick P. Stein, *Network Centric Warfare. Developing and Leveraging Information Superiority*, Washington 2000, sowie Paul T. Mitchell, *Network Centric Warfare and Coalition Operations. The new military operating system*, New York 2009, oder Edward A. Smith, Jr., »Network Centric Warfare. What's the point?« in: *Naval War College Review* 54, Nr. 1 (2001), S. 59-75.

27 Vgl. etwa Hunter Keeter, »Cebrowski: Joint Philosophy Fosters Network Centric Warfare« in: *Defense Daily International* 3, Nr. 24 (2002), S. 1, und Arthur K. Cebrowski, »Network Centric Warfare. An Emerging Military Response to the Information Age« in: *Military Technology* 27, Nr. 5 (2003), S. 16-22, und James R. Blaker, *Transforming Military Force. The Legacy of Arthur Cebrowski and Network Centric Warfare*, Westport 2007.

28 Vgl. David S. Alberts / John J. Garstka / Richard Hayes, *Understanding Information Age Warfare*, Fairfax 2001.

te.[29] Mit diesen Entwicklungen ging auch eine wachsende Interoperabilität der bestehenden Systeme einher, welche allein die Umsetzung der oben dargelegten Konzepte und Doktrinen zu realisieren in der Lage war. Und dieser Prozess dauert an. So möchte das US-Verteidigungsministerium künftig »jeden einzelnen Soldaten auf dem Schlachtfeld zu einem Hub in einem Netzwerk machen. Nicht weniger als ein Dutzend Geräte, die der Soldat bei sich tragen wird, sollen mit dem Netz verbunden sein«[30]. NCW entwickelte sich somit zunächst ausschließlich als inhärenter Bestandteil kinetischer Kriegsführung. Durch die Möglichkeiten der Informationstechnologie sollten die Land-, See-, Luft- und ggf. Weltraumstreitkräfte in ihren klassischen Bereichen effizienter werden und das herkömmliche Schlachtfeld dominieren. Eine Verselbständigung des netzwerkgestützten Krieges in einen Netzkrieg als eigenständiges Schlachtfeld war damals weder abzusehen noch gewünscht.[31] Dieser Schritt wurde erst durch die chinesische Reaktion auf die Erkenntnisse, welche Peking aus dem Zweiten Golfkrieg gewann, eingeleitet. Denn dort erkannte die politische Führung, dass die Operation Wüstensturm, jener »First Information War«[32], die bisherige auf die schiere personelle Größe ihrer Armee ausgerichtete Doktrin des Reichs der Mitte als wirkungslos gegenüber der auf NCW basierenden Dominanz anderer Großmächte, insbesondere der USA, auf dem konventionellen Schlachtfeld entlarvt hatte. In der Folge begann ein Transformationsprozess der Volksbefreiungsarmee, der am Leitbild der *Wangluohua*, der Vernetzung mit dem Ziel, das neue elektronisch gestützte Schlachtfeld zu beherrschen, ausgerichtet war. Handlungsleitend war die Überzeugung, der zufolge »eine überlegene Streitmacht, welche die Vorherrschaft im Bereich der Information verlöre, […] besiegt werden [würde],während eine unterlegene Streitmacht, die sich eine beherrschende Stellung in der Information sichert, siegen kann‘«[33]. Vor diesem Hintergrund erklärte der seinerzeitige Leiter der chinesischen Militärakademie ganz offen, das strategische Ziel der Volksrepublik sei *Zhixinxiquan*, die Informationsdominanz, welches, wie ein leitendes Mitglied des chinesischen Generalstabes erklärte, wiederum nur durch einen Präventivschlag im virtuellen Raum realisiert werden könne.[34] Die Lehren aus dem Golfkrieg, welcher als *Zhongda Biange*, große Umwälzung, Eingang in den chinesischen Sprachgebrauch hielt, gingen somit dahin, in die gegnerischen Systeme einzudringen und die Kriegsführung ins Netz selbst zu verlagern, um die eigene kinetische Unterlegenheit durch jene Art asymmetrischer Kriegführung zu kompensieren und in einen strategischen und taktischen Vorteil zu verwandeln. Konkrete Schritte, dies zu erreichen, waren relevante Technologien des potenziellen Gegners zu stehlen, die Sicherheitslücken ihrer elektronischen Systeme aufzudecken und sich so in die Lage zu versetzen, im Kriegsfall auf elektronischem Wege Schäden an der Heimatfront des Feindes, insbesondere an dessen kritischen Infrastruk-

29 Vgl. David S. Alberts / Richard E. Hayes: *Power to the Edge*, Fairfax 2003.
30 Clarke / Knake, World Wide War, aaO. (FN 3), S. 122.
31 Vgl. ebd. S. 62 f., S. 78 f.
32 Alan D. Campen, *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*, Fairfax 1992.
33 Clarke / Knake, World Wide War, aaO. (FN 3), S. 80.
34 Vgl. ebd.

turen, anzurichten. Durch eine derartige weitgehende Lahmlegung des hochgradig vernetzten Militärs der USA könnte es China dann auch mit den so geschwächten Truppen des Gegners auf dem kinetischen Schlachtfeld aufnehmen, etwa bei einer nicht unrealistischen Auseinandersetzung in pazifischen Gewässern.[35]

Ein Faktor, der eine originäre Folge des an globalem Marktliberalismus und komparativen Kostenvorteilen orientierten westlich-kapitalistischen Wirtschaftssystems ist, spielte China bei der Realisierung seiner Pläne dabei geradezu in die Hände. Denn vor dem Hintergrund der Produktionsverlagerungen sowie von freiwilligem (und nichtfreiwilligen) Wissens- und Technologietransfer wurde China, wie weitere asiatische Staaten, immer mehr zum Hersteller und Lieferanten zentraler Hardwarebestandteile, welche unentbehrlich für das alltägliche Funktionieren der westlichen Gesellschaften auf ziviler, ökonomischer, militärischer und administrativer Ebene sind. Motherboards haben gleichsam den Vorrang vor dem Vaterland erhalten. Die Bauteile für einen einzigen Computer etwa entstammen Lieferketten von bis zu 400 verschiedenen Unternehmen in Europa, Nordamerika, vor allem aber in Asien. Um zu verstehen, welches Risiko die im Ausland erzeugte Hardware in sich trägt, muss man sich das Manipulationspotenzial vor Augen führen, welches im Softwarebereich möglich ist, etwa in Form von sogenannten Hintertüren, welche gleichermaßen leicht wie regelmäßig in den Millionen Zeilen von Programmcodes, die die immer komplexer werdenden Anwendungen benötigen, versteckt werden. Im Zusammenspiel mit den historisch bedingten Konstruktionsschwächen des Internets, welche bis heute nicht ausgebügelt worden sind[36], ermöglichen diese den stetigen Zutritt in die Systeme angegriffener Nutzer, wobei zahlreiche Manipulationsmöglichkeiten wie etwa das Platzieren von logischen Bomben, welche beim Einsatz zur Übernahme oder zum gezielten Versagen des betroffenen Systems führen können, möglich sind. Führt man sich vor Augen, dass immer mehr Haushaltsgeräte und Geräte der Bürokommunikation per Internet gesteuert und somit zugleich über das Internet angreifbar werden, was von der Ausspionierung von Daten (etwa wenn sensible Dokumente fotokopiert und dabei zugleich an eine von einem Datenspion eingerichtete Adresse verschickt werden) bis hin zu zur physischen Zerstörung des Gerätes reicht, dann lassen sich die zunehmende Abhängigkeit der Gesellschaft und somit die Tragweite des Problems erkennen. Vielleicht ist es nur ein Fotokopierer, über den aber durchaus das Büro einer Entwicklungsabteilung oder eines Ministeriums in Brand gesetzt werden kann, vielleicht ist es aber auch ein Kraftwerk, ein Staudamm, ein Verkehrsflugzeug oder das gesamte Stromnetz eines Landes, das nach entsprechender Vorbereitung bei Bedarf mit dem sprichwörtlichen Mausklick ge- und sogar zerstört werden kann. Dass dies keineswegs utopisch ist zeigt der Umstand, dass US-Sicherheitsbehörden bereits heute zahlreiche logische Bomben im gesamten Stromnetz der USA entdeckt haben. Gleiches gilt für Vorkommnisse wie den Slammer Wurm, der 2003 zu massiven Störungen im

35 Simulationen haben bereits gezeigt, dass diese Strategie sich durchaus als erfolgreich für China erweisen könnte, da ein erzwungener Rückzug der USA aus pazifischen Gewässern durchaus realistisch sei; vgl. hierzu Clarke / Knake, World Wide War, aaO. (FN 3), S. 229-273.

36 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 108-122.

amerikanischen Stromnetz führte, sowie die erfolgreiche Aurora-Übung, mit der nachgewiesen wurde, wie leicht über unbefugte Zugriffe schwere Schäden an Generatoren bewirkt werden können.[37] Macht man sich in diesem Zusammenhang zudem bewusst, dass die (zumeist in Staaten wie China produzierten) Schaltkreise, welche auf den Chips in Computern, Routern, Servern etc. aufgetragen sind, selbst nichts anderes darstellen als in Silizium gegossene Software, so offenbart sich die Verletzlichkeit unserer hochgradig vernetzten Gesellschaft besonders deutlich.[38] Doch nicht nur zivile kritische Infrastrukturen sind gefährdet, gleiches gilt für die militärischen. So ist es technisch machbar, das hochgradig vernetzte Waffenarsenal eines Staates zu kapern und gezielt gegen jenes Land selbst zu lenken, inklusive der nichtkonventionellen Waffen aus dem ABC-Bereich. Ein gutes Beispiel hierfür liefert ein Vorfall, der sich zwischen Israel und Syrien zugetragen hat, bei welchem Israel in die Systeme der syrischen Luftabwehr eingedrungen ist und virtuell einen leeren Luftraum suggeriert hat, während gleichzeitig israelische Kampfflugzeuge nach Syrien flogen und auf dortigem Gebiet eine mutmaßliche Nuklearanlage zerstörten .[39] Eine ähnliche Strategie hatte das US-Militär jüngst auch für Aktionen gegenüber Libyen geplant.[40]Angesichts dieser gleichermaßen realen wie potenziell existenziellen Bedrohungen durch die Möglichkeiten von Cyberschlägen stellt sich die Frage, ob und inwieweit das offene, liberale Wirtschafts- und Gesellschaftsmodell des Westens in der gegenwärtigen Form aufrechterhalten werden kann. Dies gilt sowohl angesichts der nicht kontrollierbaren Auslandsproduktion von Kernstücken westlicher gesellschaftlicher Infrastruktur als auch vor dem Hintergrund der gegenwärtigen liberalen Werteideologie des Westens, welche anders als etwa das autoritäre China, individuelle wie unternehmerische Freiheit deutlich vor sicherheitsrelevante staatliche Eingriffe stellt. Eingedenk des bislang Geschilderten ergeben sich folgende Herausforderungen, welchen sich der deutsche Staat und seine Gesellschaft dringend stellen müssen. Auf militärischem Gebiet ist es erforderlich, eine Doktrin zu entwickeln, welche auf die Bedrohung Deutschlands durch einen möglichen Cyberkrieg reagiert. Hierbei müssen gleichermaßen offensive wie defensive Kapazitäten aufgebaut werden. Auf der Ebene der Zivilgesellschaft gilt es sich mit der Frage auseinanderzusetzen, ob und in welchem Umfang die bisherige Identität im Spannungsfeld von Freiheit und Sicherheit aufrechterhalten werden kann. Und bezogen auf die ökonomische Ebene schließlich muss diskutiert werden, inwieweit das liberal-kapitalistische Modell in der bisherigen Form fortbestehen kann. Es ist zu klären, wie die privaten volkswirtschaftlichen Akteure in höherem Maße

37 Vgl. ebd. S. 130 sowie 138 f.

38 Vgl. zur Problematik der Gefährdung kritischer Infrastrukturen im Cyberkrieg etwa Gaycken, Cyberwar, aaO. (FN 5), S. 108-120, sowie Clarke / Knake, World Wide War, aaO. (FN 3), S. 134-140, sowie Andress / Winterfeld, Cyber Warfare, aaO. (FN 4), S. 136ff.

39 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 17ff., sowie Gaycken, Cyberwar, aaO. (FN 5), S. 173 f.

40 Vgl. etwa Eric Schmitt / Thom Shanker, »U.S. Weighed Use Of Cyberattacks To Weaken Libya« in: *New York Times* vom 18.10.2011, S. A1.

als bisher in den Kontext der nationalen Sicherheit integriert werden können.[41] Nicht zuletzt gilt es in diesem Zusammenhang gegebenenfalls rechtliche Vorgaben auf nationaler Ebene anzupassen und im Bereich des internationalen Rechts dafür Sorge zu tragen, dass der bislang de facto nicht geregelte Bereich des Cyberkrieges durch Abkommen und Regime eingehegt oder zumindest berechenbarer gemacht wird. Welche konkreten Schwierigkeiten auf diesem Weg bestehen, aber auch welche Möglichkeiten sich anbieten, soll in den folgenden Abschnitten erörtert werden.

2. Das Cyberschlachtfeld

Obgleich die Cyberkriegführung im Wesentlichen technischer Natur ist, ist es doch der strukturelle wie ideologische Kontext, welcher den rechten Raum erst bereitet. Neben dem oben bereits erwähnten Problem der Versorgungskette gilt es vor allem die Problematik anzusprechen, welche aus der Ideologie einer Regulierung der Netzsicherheitsfrage im Bereich kritischer Infrastruktur durch Marktmechanismen resultiert.[42] Bereits im Bericht der von Präsident Clinton eingesetzten Marsh-Kommission[43], deren Ergebnisse 1997 vorgestellt wurden, wurde darauf verwiesen, dass das größte Sicherheitsrisiko für die USA in einem Internetangriff auf die kritischen Infrastrukturen des Landes bestehe und diese sich weitgehend unreguliert in privatwirtschaftlicher Hand befänden. Hierauf wurde jedoch in der folgenden Dekade lediglich so reagiert, dass allein Marktanreize als Mittel der Wahl betrachtet wurden; staatliche Eingriffe sollte es nur bei völligem Marktversagen geben und selbst für diesen Fall waren keine direkten staatlichen Regulierungen vorgesehen.[44] Selbst unter der Regierung Obama besteht dieses strukturelle Problem fort: Zwar kam es etwa zur Einrichtung eines militärischen Cyberkommandos, jedoch wurde weder eine kohärente Strategie für einen Netzkrieg noch ein umfassendes Programm zur Verteidigung des Privatsektors erarbeitet. Bis zuletzt schloss Obama wie schon seine Amtsvorgänger jegliche staatliche Regulierung im Bereich der Cybersicherheit für Privatunternehmen aus, obwohl »bereits seit mehr als einem Jahrzehnt vergeblich versucht wurde, die Sicherheitsprobleme durch Informationsaustausch und freiwillige Maßnahmen in den Griff zu bekommen«[45]. Ein Grund hierfür liegt nicht zuletzt im massiven Lobbying der Softwareindustrie, insbesondere des marktbeherrschenden Unternehmens Microsoft, für die es wesentlich billiger ist, Einfluss auf die Politik zu nehmen als effektiv in eine Absicherung ihrer Produkte zu investieren.[46] Welche Folgen die bestehenden Softwaremängel bereits ohne kriegerische Fremdeinwirkung haben können, zeigt der Fall des Zerstörers USS Yorktown, der nach einem Absturz des

41 Erste Ansätze dazu finden sich in den USA. Vgl. hierzu Artikel NSA und Provider wollen Rüstungsfirmen schützen, http://mcaf.ee/i1ynp sowie Anton Lischka, Apples Mann beim Geheimdienst, http://mcaf.ee/3e5nv (Stand jeweils 12.12.2011).
42 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 175-189.
43 Eigentlich: Presidential Commission on Critical Infrastructure Protection (PCCIP).
44 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 147-156.
45 Ebd. S. 163.
46 Vgl. ebd. S. 173, S. 188 f.

für alle relevanten Bereiche installierten Betriebssystems Windows NT manövrier- und handlungsunfähig auf dem Meer trieb.[47] Tatsächliche Angriffe indes können sich, wie zahlreiche Übungen und tatsächliche Vorkommnisse belegen, noch weitaus verheerender auswirken.[48] Speziell im zivilen Bereich, der den Großteil der kritischen Infrastrukturen betreibt, stellen die Industriekontrollsysteme (ICS) und insbesondere deren sogenannten SCADA-Systeme, welche auf Grundlage von Datenpunkten mit spezifischen Ein- und Ausgangswerten gesamte Installationen überwachen, steuern, regeln und visualisieren, wobei der Großteil der Regelung automatisch durch Fernbedienungsterminals (RTU) oder durch speicherprogrammierbare Steuerungen (SPS) erfolgt, eine kritische Größe dar. Die Systeme werden durch ihre hohe und stets weiter zunehmende Netzbasiertheit – die Kommunikation erfolgt weitgehend auf der Grundlage von (teilweise sogar drahtlosen) TCP-Techniken, welche als »primary security threat posed by the internet«[49] bewertet werden – in besonderem Maße verletzlich. Dies gilt umso mehr, weil entsprechende SCADA-Pläne nicht selten regulär im Internet abrufbar sind.[50] Wie zentral SCADAs in heutigen Systemen sind und wie weitreichend die Folgen unbeabsichtigter oder vorsätzlich herbeigeführter Ausfälle sein können, haben mehrere Fälle gezeigt. So führte etwa im August 2003 der Ausfall in einem Softwareüberwachungssystem in einem hierfür zuständigen Betrieb in Ohio zur Abschaltung eines örtlichen Kraftwerks, was eine Kettenreaktion nach sich zog, in deren Rahmen aufgrund der Selbststabilisierungsversuche des Systems schließlich 256 Kraftwerke im gesamten Nordosten der USA und in Teilen von Kanada vom Netz getrennt wurden, sodass etwa 55 Millionen Menschen ohne Stromversorgung waren.[51] Als Folge einer vorsätzlichen Manipulation der Programmcodes für die automatisierte Pumpen- und Ventilsteuerung einer sowjetischen Transkontinentalpipeline kam es zur größten bislang registrierten nichtnuklearen Explosion mit einer Sprengkraft von mehr als drei Kilotonnen nachdem in einem Abschnitt der Pipeline das manipulierte Programm der Pumpe an dem einen Ende den Befehl erteilte, die Durchflussrate zu maximieren, während sie gleichzeitig das Ventil auf der anderen Seite schloss.[52] Ein jüngeres Beispiel ist der Stuxnet-Angriff von

47 Vgl. ebd. S. 186.

48 Vgl. etwa Craig Wright, »Lebensgefahr aus dem Internet« in: *Die Zeit* Nr. 42 (2011), S. 26.

49 Kelly A. Gable, »Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent« in: *Vanderbilt Journal of Transnational Law*, 34 (2010), S. 57-118, hier S. 64. Zur genauen Funktionsweise und dem daraus erwachsenden Gefahrenpotenzial von TCP vgl. ebd. S. 78ff. sowie speziell für die kritische Infrastruktur Finanzsektor S. 84ff.

50 Vgl. z.B. http://mcaf.ee/q86ve (Stand 12.12.2011).

51 Vgl. Andress / Winterfeld, Cyber Warfare, aaO. (FN 4), S. 125 f.

52 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 131. Die Sowjetunion hatte versucht, den Programmcode bei einem kanadischen Unternehmen zu stehlen, was jedoch bemerkt wurde. Der kanadische und der US-amerikanische Geheimdienst versahen die Software daraufhin bewusst mit Fehlern und ließen die Sowjets im Glauben, unbemerkt eine funktionierende Software gestohlen zu haben.

2009.[53] Das Zielobjekt des Stuxnet-Wurms war WinCC-S7, eine weltweit eingesetzte Standardsoftware von Siemens zur automatischen Überwachung und Steuerung wichtiger Bestandteile von Stromnetzen. Stuxnet war als multiple Zero-Day-Attacke bis dahin nie gekannter Komplexität mit immensem Aufwand programmiert worden, ein Umstand der darauf hindeutet, dass ein oder mehrere Staaten (hier mutmaßlich die USA und Israel) hinter dem Projekt standen. Ziel des Angriffs war die iranische Urananreicherungsanlage von Natanz, deren Zentrifugen mit WinCC-S7 gesteuert wurden. Der Stuxnet-Wurm drang in die Siemens-Software ein und änderte die Befehle, die den Zentrifugen erteilt worden, mit dem Resultat, dass die elektrischen Motoren auf eine Weise oszillierten, dass eine Urananreicherung verhindert wurde.[54] Was die Bedeutung jener Attacke anbelangt, so hat man bei Stuxnet »gesehen, was passiert, wenn sich ein paar Leute zusammensetzen und mal richtig viel Zeit und Geld investieren, um eine effektive Cyberwaffe zu schmieden. Das ist aber nur ein Vorgeschmack. «[55] Denn genauso wie man vom Cyberspace aus das Stromnetz abzuschalten oder einen Generator beschädigen kann, ist es möglich Züge zum Entgleisen und Flugzeuge zum Absturz zu bringen, Gütertransporte an falsche Bestimmungsorte zu leiten oder Waffensysteme zu manipulieren. Daher ist es wichtig, sich kurz die Ablaufweise eines Cyberangriffs zu vergegenwärtigen, um zu sehen, wie Verteidigungsmaßnahmen aussehen und wo sie angesetzt werden müssen.

Angriffe aus dem Cyberspace verlaufen modellhaft nach einem spezifischen Muster.[56] Einer Cyberattacke gehen zunächst Maßnahmen der Aufklärung (*Reconnaissance*) voraus, die sowohl technische (*Computer Network Exploitation,* CNE) als auch menschliche Komponenten (*Social Engineering,* SE) beinhalten. Hierbei kann das SE verstanden werden als »act of influencing someone's behavior through manipulating their memories, or gaining and betraying their trust to gain access to their system. This can be done in person, over the phone, via an email, through social media, or a variety of other methods«[57] . Während SE in seiner allgemeinen Variante als groß angelegtes Password-Phishing auftreten kann, sind auch Aktionen gegenüber ausgewählten Individuen möglich, um deren Gewohnheiten etc. zu erfahren. CNE greift sowohl auf offene Quellen (*Open Source Intelligence*, OSINT) als auch auf gezielte technische Überwachungsmaßnahmen zurück, wobei regelmäßig spezielle Programme und Methoden wie Port Scans, Fingerprint OS, Vulnerability Assessment, Whois, Maltego oder Deep-Web-Suchmaschinen

53 Vgl. etwa John Richardson, *Stuxnet as Cyberwarfare. Distinction and Proportionalirty on the Cyber Battlefield*, Washington 2011, sowie Paul K. Kerr / John Rollins / Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Washington 2010, sowie James P. Farwell / Rafal Rohozinski, »Stuxnet and the Future of Cyber War« in: *Survival* 53, Nr. 1 (2011), S. 23-40, sowie Thomas N. Chen,»Stuxnet. The Real Start of Cyberwarfare« in: *IEEE Network*, Nr. 6 (2010), S. 2 f.

54 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 50-56.

55 Tagesschau-Interview *Stuxnet-Virus ist nur ein Vorgeschmack* mit Wolfgang Stieler vom 14.10.2010, http://mcaf.ee/wht80 (Stand 27.10.2011).

56 Vgl. zu den Schritten sowie den damit zusammenhängenden Einzelmaßnahmen Andress / Winterfeld, Cyber Warfare, aaO. (FN 4), S. 83-118, 139-166 und S. 170-178. Vgl. ausführlich zur Verwundbarkeit vernetzter Systeme ferner Steven Furnell, *Computer Insecurity. Risking the System*, London 2005.

57 Andress, / Winterfeld, aaO. (FN 4) S. 139.

sowie Metadatenanalysetools wie Metagoofil oder Exitfool zur Anwendung kommen. Die hierbei gewonnenen Erkenntnisse, in der Regel erste Passwörter, werden in einem weiteren Schritt (*Scan*) genutzt, um im System nach nun detaillierteren Informationen zur Zielumgebung selbst zu suchen, wobei besonders verwundbare Bereiche wie das Verbindungsglied zwischen Datenbank und Internetstelle von besonderem Interesse sind. Hierbei kommen Tools wie Nmap oder Nessus zur Anwendung, welche in besonderer Weise geeignet sind, Schwachstellen von Systemen, vor allem auf dem Gebiet der oben näher behandelten SCADAs, aufzudecken.[58] Ist das zu manipulierende Betriebssystem näher ausgekundschaftet, wird versucht, die eigenen Berechtigungen horizontal wie vertikal weiter auszubauen (*Access & Escalation*), etwa durch Zugriff auf weitere Benutzerkonten einer gleichwertigen Berechtigungsstufe beziehungsweise auf solche mit höheren Befugnissen, wie Administratorkonten. Hierbei kommen Passwort-Tools wie Hydra oder Metasploit-Instrumente zum Einsatz. Hat man bestimmte Bereiche des Netzwerks auf diese Weise unter seine Kontrolle gebracht, ist es etwa möglich mit Hilfe des FTP, des SCP oder des XMPP[59] Daten zu entführen (*Exfiltration*). Auf diese Weise kann sowohl die Vertrauenswürdigkeit als auch die Verfügbarkeitsfunktion eines Systems kompromittiert werden. Ferner ermöglich ein derartiger Zugriff auf das System auch den Bereich der Datenintegrität zu beeinträchtigen (*Assault*), etwa indem Daten oder Prozesse gezielt manipuliert werden, sodass falsche Daten auf Anzeigen erscheinen, wie dies etwa im Fall der oben beschrieben Operation Orchard bei den syrischen Radaranlagen der Fall war. Um dem Angreifer einen dauerhaften Zugriff zu gewährleisten, kann er mit den erlangten Berechtigungen Hintertüren schaffen, neue Konten kreieren, eigene Command-and-Control-Instrumente einrichten oder das System beliebig rekonfigurieren. Auch ist es ihm möglich, die eigenen Spuren seines Eindringens ins System zu verwischen oder bewusst falsche Fährten zu legen, die etwa auf einen dritten Staat als Eindringling hinweisen (*Obfuscation*). Dieser Punkt verweist auf ein weiteres zentrales Problem, nämlich die Zurechenbarkeit von Angriffen (*Attribution*), das sich etwa bei den Konflikten zwischen Russland und Estland beziehungsweise Russland und Georgien gezeigt hat.[60]

3. Umgang mit den Herausforderungen des Cyberkrieges

Insgesamt lassen sich somit vier Bereiche erkennen, auf denen auf die Herausforderungen, welche sich durch die neue Art der Kriegführung ergeben, reagiert werden muss, nämlich der technisch-organisatorische, der politisch-militärische, der juristische und der gesellschaftliche. Der erste Bereich fokussiert dabei auf die technischen beziehungsweise

58 Vgl. etwa Gordon 'Fyodor' Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*, Sunnyvale 2008.

59 FTP = File Transfer Protocol, SCP = Secure Copy Protocol, XMPP = Extensible Messaging and Presence Protocol; vgl. hierzu etwa http://tools.ietf.org/html/rfc959, http://mcaf.ee/r2yea, http://mcaf.ee/tkoxi und http://mcaf.ee/rfuny (Stand jeweils 13.12.2011).

60 Vgl. hierzu etwa Clarke / Knake, World Wide War, aaO. (FN 3), S. 29-40, sowie Gaycken, Cyberwar, aaO. (FN 5), S. 169-173.

organisatorischen Möglichkeiten und Defizite, welche zur Verteidigung netzbasierter Systeme existieren. Der zweite Bereich betrifft die Entwicklung einer militärischen Doktrin für den Cyberkrieg, welche strategische und taktische Überlegungen sowohl im prozessualen als auch im institutionellen Bereich beinhaltet. Die juristische Ebene zielt auf relevante Regelungen im nationalen Recht sowie im Bereich des Völkerrechts und die letzte Ebene umfasst Fragen, wie die Gesellschaft als Ganzes auf die Herausforderung Cyberkrieg reagieren kann.

3.1 Technisch-organisatorischer Bereich: Aspekte der Computer Network Defense (CND)

Eine grundlegende Herausforderung gerade auf technischer Ebene besteht darin, dass die »meisten Verteidigungskonzepte im Bereich Cyberwarfare mit unüberwindbaren systemischen Problemen behaftet«[61] sind. Diese Tatsache ist umso gravierender, weil es sich beim zu schützenden Gut um hochsensible Daten wie Steuerungscodes für sensible Anlagen, geheime Baupläne oder strategische Operationspläne aus dem militärischen Bereich handelt. Bei der Gestaltung von Abwehrmaßnahmen müssen somit drei Ziele erreicht werden[62]: Erstens die Wahrung der Vertraulichkeit der Daten (*Confidentiality*), etwa über Zugangskontrollen und Verschlüsselung, sodass der Diebstahl hochsensibler Daten wie etwa in jenem Fall, wo die Bau- und Technikpläne des mehrere Hundertmilliarden Dollar schweren für die nationale Sicherheit als äußerst wichtig eingestuften F-35 Kampflugzeugprojektes, das aufgrund seiner neuen Technologien SA und NATO eine Dominanz auf etwa drei Jahrzehnte hinaus sichern sollte, gestohlen wurden[63], verhindert wird. Zweitens mithilfe ähnlicher Instrumente wie oben sowie sogenannter Mashes und Message Digests[64] der Schutz der Integrität von Daten (*Integrity*), sodass es zu keinen Manipulationen kommen kann wie etwa bei der erwähnten Operation Orchard. Und drittens die Gewährleistung der Verfügbarkeit von Daten (*Availability*), sodass ein Zugriff stets erfolgen kann, wenn dies gewünscht ist. Dies erfordert insbesondere die Schaffung einer Umgebung, die stabil genug ist, um mit Strom-, Kommunikations- und Systemausfällen fertig zu werden, was vor allem mithilfe von Redundanzen und Backups erfolgt. Grundsätzlich ist es unabdingbar, mit größter Sorgfalt bestimmte Standardmaßnahmen wie Update-Management, Malware-Scanner, Firewalls, Authentifizierungssysteme und Verschlüsselungen implementiert zu haben, welche zudem im Rahmen der sogenannten mehrfach geschichteten Verteidigung (*Layered Defense*) miteinander kom-

61 Gaycken, Cyberwar, aaO. (FN 5), S. 152.

62 Vgl. zu den nachfolgend erwähnten Maßnahmen etc. ebd. S. 155-166, und Andress / Winterfeld, aaO. (FN 4), S. 182-190.

63 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 290-293. Im genannten Fall wurden mehrere Terabyte hochsensibler Daten gestohlen, eine Menge, welche mehreren hundert Millionen Wörtern entspricht.

64 Hierunter werden spezifische kryptografische Protokolle bezeichnet, deren Eigenschaft es ist, dass weder aus dem verschlüsselten Text der Originaltext wieder hergestellt werden kann (keine Umkehrbarkeit), noch dass ein Text berechnet werden kann, der das gleiche Chiffrat wie der Originaltext erzeugt (keine Kollision).

biniert werden[65], sodass ähnlich wie bei einem mittelalterlichen Burgwall mehrere Verteidigungslinien überwunden werden müssen. Obgleich Best Practice für den technischen Teil der direkten Abwehr, hilft auch dieses System nur bedingt und kann Attacken bestenfalls verlangsamen, nicht jedoch aufhalten. Umso wichtiger ist daher die Erlangung von Widerstandsfähigkeit im System, was bedeutet, dass die Schäden nach einem erfolgreichen Angriff minimiert werden, etwa indem Folgeschritte vereitelt werden (*Mitigation*), Ersatzsysteme die Operationen weiterführen (*Continuity*) oder die betroffenen Systeme selbst möglichst schnell wieder in Betrieb gehen können (*Recovery*). Neben Redundanzen ist die Modularisierung von Systemen das Mittel der Wahl (Individualisierung). Kombiniert mit dem Konzept der geschichteten Verteidigung ermöglicht eine solche Individualisierung einen Ansatz multipler unabhängiger Sicherheitsebenen (*Multiple Independent Layers of Security*). Nicht weniger bedeutsam als die technischen Vorkehrungen sind Maßnahmen der Sensibilisierung und des Trainings der Betreiber und Anwender von Software und Datennetzen. Vor dem Hintergrund der bisherigen Analyse stellt sich die Frage, wie eine entsprechende Militärdoktrin aussehen sollte, welche die bisher gewonnenen Erkenntnisse berücksichtigt.

3.2 Militärischer Bereich: Wesen des Cyberkrieges und Folgen für die Doktrinentwicklung

Der Cyberkrieg wurde nicht zu Unrecht als »terra nullius«[66] beschreiben und stellt gerade daher für die Streitkräfte eine bedeutende Herausforderung dar. Dies liegt nicht zuletzt daran, dass auch die westlichen militärischen Eliten die Bedrohung durch den Cyberkrieg unterschätzen und die entsprechende Technologie eher sehen »als Ass im Ärmel, als etwas dass dafür sorgt, dass unsere Flugzeuge, Schiffe und Panzer besser funktionieren als anderen auf der Welt. Den meisten fällt die Vorstellung schwer, dass andere Nationen Technologie effektiv gegen uns einsetzen können, vor allem, wenn es sich bei dieser Technik nicht um einen Tarnkappenbomber, sondern um einen […] Programmcode handelt. «[67] Eine besondere Herausforderung ist der Umstand, dass jedoch genau auf diese Weise kleine, auf konventionellem Gebiet schwache Staaten, unverhältnismäßig viel an Macht gewinnen. Dies gilt umso mehr, da der Cyberkrieg beziehungsweise dessen Vorbereitung weitgehend stillschweigend und anonym ablaufen kann. Der Cyberkrieg ist ferner von einer Entterritorialisierung sowie einer zusehenden Vermischung von privaten und öffentlichen, zivilen und militärischen Strukturen und Prozessen gekennzeichnet. Angesichts dieser Tatsachen hat sich der Cyberkrieg zu einem eigenständigen fünften Schlachtfeld neben den Bereichen Land, See, Luft und Weltraum entwickelt, dessen spezifische Charakteristika nicht ohne Folgen für eine Doktrinentwicklung sind. Entscheidende Probleme, die sich in diesem Kontext ergeben, sind die

65 Etwa in Form von Firewalls und IDS/IPS auf der Netzwerkebene, Softwarefirewalls und Anti-Malware-Tools auf der Host-Ebene, Zugangskontrollen auf der Anwendungsebene und Verschlüsselung auf der Daten-Ebene.

66 Paul Cornish / David Livingstone / Dave Clemente / Claire Yorke, *On Cyber Warfare. A Chatham House Report*, London 2010, S. vii.

67 Clarke, / Knake, World Wide War, aaO. (FN 3), S. 246 f.

Zurechenbarkeit von Angriffen (*Attribution*), die Möglichkeit von Abschreckung, die Frage nach dem Erstschlag und die Gefahr einer Eskalation. Wie weiter oben dargelegt ist es für Angreifer möglich, ihre Spuren zu verwischen oder aber dafür zu sorgen, dass die Spuren des Angriffs in ein anderes Land weisen, als dasjenige von welchem die Attacke tatsächlich ausgegangen ist. Auf diese Weise besteht die Gefahr, dass an sich unbeteiligte Staaten in Konflikte hineingezogen werden, etwa wenn Cyberangriffe ohne deren Wissen über Server gelaufen sind, welche sich auf dem Territorium jener Drittstaaten befanden und diese Länder dann aber von Vergeltungsmaßnahmen des Verteidigers getroffen werden. Es gibt sogar Vorschläge, welche bewusst in diese Richtung gehen, wie etwa die Möglichkeit der Anwendung der Safe-Haven-Regelung des Kriegsrechts auf Cyberangriffe, sodass Staaten angegriffen werden dürfen, die nicht in der Lage sind, (nicht-staatliche) Hackerangriffe, welche über ihr Territorium laufen, zu unterbinden.[68] Auch wenn dieser Ansatz drastisch und aus Sicht des internationalen Rechts nicht unproblematisch sein dürfte, trifft er doch eine offene Flanke. Denn natürlich ist die Möglichkeit, Gegenmaßnahmen vis-à-vis einem Angreifer zu ergreifen, in einem Konflikt essenziell. Das Problem ist, dass die Attribution im Kontext des Cyberwars der Non-Attribution gewichen ist.[69] Was das für die Entwicklung einer Doktrin bedeutet, hat William Lynn vom US-Verteidigungsministerium 2010 erklärt: »[W]e have to shift our cyber defence paradigm from assured retaliation to denial of benefit«[70].

Da, wie aufgezeigt, keine endgültig sicheren technischen und organisatorischen Wege existieren, sich ultimativ gegen Cyberangriffe zu schützen, wäre Abschreckung die zwingende alternative Handlungsoption. Kennt man den Angreifer indes nicht, wird Abschreckung sehr schwer. Aber die Nicht-Attribution ist nicht die einzige Schwierigkeit, die im Zusammenhang mit Abschreckung besteht.[71] Ein grundsätzliches Problem liegt darin begründet, dass der Faktor Abschreckung in der gegenwärtigen Cyberkriegstheorie nur wenig entwickelt ist und auch Anleihen etwa bei Konzepten der Nuklearstrategie kaum möglich sind. Denn während die atomare Abschreckung auf den bekannten gravierenden Effekten des Einsatzes einer Nuklearwaffe beruhte – die gleichsam garantierte Zerstörung des Angreifers beim atomaren Gegenschlag sowie die äußerst wahrscheinliche weitgehende Auslöschung der Menschheit durch den folgenden nuklearen Winter – sind die Folgen eines umfassenden Cyberkrieges weder klar noch bekannt. Hinzu kommt, dass bereits erfolgte Cyberattacken bislang kaum breite öffentliche Resonanz erfahren haben, ja in manchen Fällen lange nicht einmal vom Angegriffenen bemerkt wurden, falls dies überhaupt geschehen ist. Nicht zuletzt kann anders als im kinetischen Bereich, die Funktionsweise hoch entwickelter Cyberwaffen nicht einfach demonstriert werden, weil ein Einsatz häufig nur einmal möglich ist. Denn wurde eine Cyberwaffe

68 Vgl. etwa Matthew Sklerov, »Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Which Neglect Their Duty to Prevent« in: *Military Law Review*, Nr. 201 (2009), S. 1-85.

69 Vgl. Gaycken, Cyber Warfare, aaO. (FN 5), S. 80ff.

70 SDA (Hg.): *A Conversation on Cyber Security*. Brüssel 2010, S. 3.

71 Vgl. Clarke / Knake, World Wide War, aaO. (FN 3), S. 240ff, und Gaycken, Cyberwar, aaO. (FN 5), S. 149ff.

erst einmal offenbart, können Gegenmaßnahmen gegen den Mechanismus entwickelt und die erkannten Sicherheitslücken bestehender Systeme geschlossen werden. Aus den mangelnden Erfahrungswerten resultiert zwar die Unsicherheit, nicht zu wissen, ob die Rückschlagkapazitäten und Reaktionen eines angegriffenen Gegners nicht ganz anders liegen als erwartet: Würden die eigenen Pläne noch funktionieren, wenn der Gegner sich über einen Notschalter (*Kill Switch*) vom Internet abkoppeln würde oder wäre es sichergestellt, dass einst platzierte logische Bomben nicht längst entdeckt und unschädlich gemacht sind? Ein Luftangriff, der mit einem lahmgelegten Radarsystem der Verteidiger rechnet, könnte davon überrascht werden, dass dieses aufgrund der vorausgegangenen Entschärfung der logischen Bomben doch funktioniert, ja der Angreifer könnte sogar mit falschen Daten konfrontiert sein, weil in dessen System hinterlegte logische Bomben vom Verteidiger aktiviert werden. Sicher jedoch ist nichts und daher ist angesichts der oben erwähnten Einstellung vieler Militärs, welche nach wie vor davon ausgehen, dass der NCW den westlichen Staaten eine dominante Position auch auf den heutigen Schlachtfeldern verleiht, davon auszugehen, dass die Bedrohung durch Cyberwaffen im Ernstfall nicht abschreckend auf die Entscheidung wirkt, eine kinetische Kriegshandlung einzuleiten.[72] Wie oben beschrieben, bleibt somit nur die Möglichkeit, die Systeme so zu gestalten, dass ein Angriff einen minimal möglichen Schaden anrichtet, während die eigene Erstschlagfähigkeit maximiert wird. Entscheidend bei der Bewertung des Erstschlages ist das Phänomen des First Mover Advantage, demzufolge der Vorteil bei dem Akteur liegt, welcher zuerst handelt. Denn wer im Cyberspace nicht zuerst agiert, dem kann die Fähigkeit zum Angriff und zur Verteidigung von der Gegenseite blockiert werden, etwa indem der Gegner seine Netze von der Außenwelt abkoppelt und zugleich Maßnahmen der offensiven Cyberkriegführung, etwa die Zerstörung ausgewählter kritischer Infrastrukturen, allen voran die Telekommunikations- und Stromnetze, einleitet. Der beschriebene Vorteil des zuerst handelnden Akteurs ist geeignet, die Instabilität in einer Krisensituation zu erhöhen, da sie einen erheblichen Druck auf die Entscheidungsverantwortlichen aufbaut. Das gilt umso mehr, da sie in kritischen Situationen diese vor dem Hintergrund der zu erwartenden konstruktiven Ambiguität interpretieren müssen, also damit konfrontiert sind, dass Verlautbarungen und Handeln eines Staates gegebenenfalls nicht übereinstimmen. Wenn ein Akteur dann davon ausgeht, dass die Gegenseite seine kritische Infrastruktur bereits mit Schadprogrammen oder logischen Bomben infiziert hat, kann diese Annahme in Kombination mit dem First-Mover-Advantage den Entscheidungsträger in Zeiten der Anspannung geneigt machen, einen Cyberangriff zu veranlassen.[73] Die Gefahr einer weiteren Kriseneskalation besteht zudem bei Cyberangriffen, welche die Kommando- und Kontrollstrukturen des Gegners allzu umfassend außer Kraft setzen einerseits, sowie durch die Folgen der auf die Perzeption des Gegners hin ausgerichtete Art der Kriegführung, bei der die Systemdaten manipuliert werden

72 Zu diesem Ergebnis kommt auch die Simulation eines Konfliktes zwischen den USA und China im Südchinesischen Meer, welche von Clarke / Knake, World Wide War, aaO. (FN 3), S. 246, beschrieben wird.

73 Vgl. ebd. S. 249, 253, 271 f.

andererseits. Im ersten Fall kann es passieren, dass etwa das gegnerische Oberkommando möglicherweise nicht einmal mehr die Einstellung der Kampfhandlungen befehlen kann. Zugleich könnte aber auch ein lokaler Kommandeur, der solche Befehle erhält, davon ausgehen, diese seien vom Gegner ins System geschleust, und stattdessen in die Offensive gehen. Somit besteht die Gefahr eines weitgehenden Kontrollverlusts über die Kampfhandlungen auf beiden Seiten.[74] Es ist daher in jedem Fall zu verhindern, dass der Gegner völlig enthauptet wird. Dies kann jedoch gegenwärtig keinen völligen Verzicht des auch initiativen Einsatzes von Cyberwaffen rechtfertigen. Denn ein bewusster, namentlich einseitig avisierter Verzicht auf einen Erstschlag würde notwendigerweise den Verzicht auf die Unterstützung kinetischer Angriffe bedeuten, sodass diese – zumindest wenn man mögliche effektive Abwehrmaßnahmen außen vor lässt – weniger effizient ablaufen würden, was zu einem unnötigen Mehraufwand an Mensch und Material und möglichen höheren Verlusten dieser Faktoren führen würde. In jedem Fall würde man taktische wie strategische Vorteile preisgeben.[75] Somit ist der Verzicht auf die Erstschlagmöglichkeit zunächst einmal nicht zu erwägen. Dass jedoch auch hierbei Gebote wie Zurückhaltung und Verhältnismäßigkeit zu beachten sind ergibt sich ebenso aus militärischer Logik, politischem Kalkül und nicht zuletzt der Sphäre des Rechts.

3.3 Juristischer Bereich: (Inter-)Nationale Regelung der Anarchie im Cyberspace

Bei dieser Betrachtung soll allerdings nicht um eine Analyse von Fragen der Anwendbarkeit bzw. Übertragbarkeit konkreter bestehender Rechtsnormen, etwa des internationalen See- oder Weltraumrechts, gehen oder die Varianten von *ius ad bellum*, *ius in bello* und *ius post bellum* im Kontext von Cyberwar analysiert werden.[76] Ebenso wenig kann es an dieser Stelle um eine ausführliche Überprüfung von Wirksamkeit oder Übertragbarkeit spezifischer nationaler Regelungen gehen.[77] Vielmehr sollen hier kurz einige Überlegungen aus dem juristischen Bereich beleuchtet werden, welche für Politik und Gesellschaft – namentlich die deutsche – ihrem Gesamtprinzip nach von Relevanz sind und dort den Diskurs initiieren und vorantreiben können.[78] Auf Ebene des Völkerrechts stellt sich die Frage nach internationalen Abkommen und Regimen. Die Beurteilung der

74 Vgl. ebd. S. 259-264.

75 Vgl. ebd. S. 248.

76 Vgl. zu diesen Themenbereichen etwa Scott Shackelford, »From Nuclear War to Net War: Analogizing Cyber Attacks in International Law« in: *Berkeley Journal of International Law*, Vol. 27, No. 1 (2009), S. 191-251, sowie Michael N. Schmitt, *»Wired Warfare: Computer network attack an jus in bello«* in: *IRRC* 84, Nr. 864 (2002), S. 365-399, sowie Thomas C. Wingfield, *»International Law and Information Operations«* in: Franklin D. Kramer / Stuart H. Starr / Larry K. Wentz (Hg.): *Cyberpower and National Security*, Dulles 2009, S. 525-542, sowie Kelly A. Gable, »Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent«, in: *Vanderbilt Journal of Transnational Law*, 43 (2009), S. 57-118.

77 Vgl. vor allem für den Bereich der USA etwa Andress / Winterfeld, Cyber Warfare, aaO. (FN 4), S. 213ff.

78 Vgl. hierzu etwa Clarke / Knake, aaO (FN 3), S. 296-314.

Sinnhaftigkeit einer solchen Institution hängt dabei maßgeblich von der bestehenden Doktrin ab. Problematisch ist hier unter anderem für Deutschland, dass eine solche derzeit nicht existiert. Somit lässt sich nicht beurteilen, ob ein spezifisch ausgearbeitetes Rüstungsabkommen für den Cyberspace, dem eigenen Land zum Vor- oder Nachteil gereicht. Hinzu kommt eine Vielzahl praktischer Schwierigkeiten wenn es um die Frage nach einem internationalen vertraglich geregeltem Verbot des Cyberkrieges geht. Ein vollständiges Verbot wäre zwar theoretisch möglich und vielleicht auch wünschenswert, jedoch ist es mit den derzeitigen Mitteln weder prüfbar noch durchsetzbar. Hinzu tritt das oben geschilderte ungelöste Problem des First Mover Advantage. Ein umfassendes Angriffsverbot, welches zwar den Einsatz von Cyberwaffen im Kriegsfall billigt, jedoch einen Ersteinsatz verbietet, um so zu verhindern, dass sich aus ihrem Einsatz überhaupt erst ein kinetischer Krieg entwickelt, erscheint realistischer, da eine international geachtete normative Grenze überschritten würde, was zu Sanktionen, Ächtung und Verlust von Verbündeten führen könnte. Für die im vorliegenden Beitrag betrachteten hochgradig vernetzten westlichen Gesellschaften wäre auch ein selektives Angriffsverbot von Vorteil, das Angriffe auf Zivilisten, i.e. zivile Infrastrukturen unterbinden würde. Da diese Staaten im Defensivbereich zurückliegen, könnten sie so ihre NCW-Kapazitäten besser ausspielen. Allerdings wären auch hier Umsetzung und Kontrollen schwierig, und ohne Kontrollen wäre letztlich nur ein sehr weiches Regime zu erwarten. Hilfreich wäre auch ein Ansatz, der alle Staaten in die Pflicht nähme, zu unterbinden, dass über deren System Angriffe laufen. Dies umginge auch das Problem der Zurechenbarkeit, weil jeder in der Verantwortung steht, unabhängig davon, ob er intentionale Schuld aufweist. Sanktioniert werden könnte eine Nichtbeachtung etwa durch ein Schwarze-Liste-System, bei dem, sobald ein Land darin enthalten ist, dieses vom Internet getrennt wird. Ob es hierfür jedoch genügend Unterzeichner gibt, zumal viele Staaten die technischen Voraussetzungen hierfür nicht einmal ansatzweise erfüllen, ist fraglich. Worum es daher im Augenblick geht ist die Reduzierung von Fehleinschätzungen. Im Grund muss das alte Problem der Internationalen Beziehungen (IB), das sogenannte Sicherheitsdilemma, welches durch den Cyberkrieg in einem neuen Gewand daherkommt, aufs Neue überwunden werden, vor allem mit den klassischen Ansätzen der IB-Lehre und der Politischen Psychologie, wie etwa verfestigten Kommunikationskanälen, vertrauensbildenden Maßnahmen und der Schaffung von Transparenz. Das wohl größte Problem in diesem Zusammenhang ist das Konterkarieren ebendieser Maßnahmen durch die quantitativ wie qualitativ zunehmende Cyberspionage, die zudem leichter, gefahrloser, effizienter und weniger leicht zu entdecken ist als die traditionelle Weise. Hierunter hat das Vertrauen zwischen den Staaten zuletzt in hohem Maße gelitten. Nicht zuletzt vor diesem Hintergrund ist ein Ausbau der eigenen Offensiv- und Defensivkapazitäten zur Sicherstellung der eigenen nationalen Sicherheit unabdingbar. Denn derzeit gleicht das Internet einer Domäne in welcher der hobbesianische Urzustand herrscht. Dieser Umstand hat auch unmittelbare Bedeutung für den Bereich des nationalen Rechts. Wie dargestellt hat sich gezeigt, wie gefährlich ein Vertrauen auf die reine Selbstregulation des Marktes im Bereich kritischer Infrastrukturen ist. Daher gilt es, Abstand zu nehmen vom Modell des ungezügelten Marktvertrauens, ebenso wie dies auch in anderen Bereichen wie dem Finanzsektor immer dringlicher wird.

Soll die Sicherheit von Staat, Wirtschaft und Gesellschaft künftig gewahrt werden, so kann auf staatliche Regulierung zentraler Bereiche der Privatwirtschaft westlicher Staaten in weit höherem Maße als bislang nicht verzichtet werden. Dies gilt für den systemrelevanten Bankensektor, der bei Vertrauensverlusten, die leicht die Folge von Cyberangriffen sein können, ganze Volkswirtschaften gefährden kann, und zwar in einer Weise, welche alle bisherigen Krisen weit in den Schatten zu stellen in der Lage wäre, ferner für die Stromnetze, wo der alte Werbeslogan *Im Prinzip geht alles aber ohne Strom läuft nichts* die bittere Quintessenz der Verletzlichkeit kritischer Infrastrukturen durch Cyberkrieg pointiert in Worte kleidet und schließlich die Basisnetze eines Landes, welche, obgleich nur eine Handvoll, regelmäßig etwa 90% des Datenverkehrs eines Landes abwickeln. Wäre es möglich einen Angriff dort abzufangen, würde er das eigentliche Zielnetz mit hoher Wahrscheinlichkeit nicht erreichen. Technisch wäre dies etwa im Rahmen einer latenzfreien Deep-Packet Inspection möglich, jedoch stehen häufig datenschutzrechtliche Regelungen einer effizienten Prüfung entgegen, weil viele Wirtschaftsunternehmen, auch wenn sie es könnten, selbst bei erkennbaren Gefährdungen nicht eingreifen aus Angst Kunden zu verlieren oder wegen Datenschutzverletzungen verklagt zu werden. Dieser Zustand muss durch gesetzliche Regelungen beendet werden, sodass eine Prüfungs- und Handlungs*pflicht* für die Provider besteht und sie auf einer rechtlich abgesicherten Position stehen. Was an dieser Stelle eklatant zu Tage tritt ist ein höchst problematisches Grundwerteverständnis. Mit anderen Worten steht der Grundwert Datenschutz nicht in einem gesunden Verhältnis zu anderen Grundwerten. Ein neuer Konsens ist nötig, der das Recht auf Leben und körperliche Unversehrtheit höher bewertet als das Recht auf informationelle Selbstbestimmung, nicht zuletzt will diese nicht selten durch die Bürger selbst leichtfertig missachtet wird und diese so nicht unerheblich an der Gefährdung der nationalen Sicherheit mitwirken. Zudem ist problematisch, dass sich Kontrollmechanismen nicht so sehr gegen diejenigen richten, die tatsächlich darauf aus sind, die nationale Sicherheit zu gefährden, sondern gegen jene, deren originäre Aufgabe es ist, die Freiheit und Sicherheit der BürgerInnen zu gewährleisten. Auch hier sind Gesetzesanpassungen erforderlich, sodass Cyberkrieger nicht länger von Regeln profitieren und geschützt werden, die lediglich einer spezifischen Ideologie folgen, welche ebenso naiv wie fehlgeleitet ist– zum Nachteil der gesamten Gesellschaft. Zudem muss die Güterabwägung auch in einem anderen Bereich im oben genannten Sinne angepasst werden: Bei der Gefahrenabwehr im Cyberkrieg müssen Entscheidungen ohne jegliche Verzögerung getroffen werden können um überhaupt eine Chance zu haben. Die Abwägung hat somit im Vorfeld zu erfolgen, sodass die operativen Prozesse im Handlungsfall gemäß Standardverfahrensweisen ablaufen können. Ein wesentliches Problem auf juristischem Gebiet ist dabei das Fehlen der geeigneten juristischen Instrumente, ein Mangel an Sachverstand für die Sachfragen jenseits des juristischen Handwerkszeugs, i.e. für die komplexen Herausforderungen des Cyberspace, was jedoch unmittelbar auf die originär juristischen wie pragmatischen Möglichkeiten zurückschlägt, und nicht selten der fehlende Wille in neuen Bahnen zu denken.[79] Auch hieran muss gearbeitet werden, soll nicht das

79 Vgl. hierzu Kriesel / Kriesel, Cyberwar, aaO (FN 7), S. 210ff.

Gesellschaftsmodell an ignoranten Ideologen und einer selbstgerechten, weltfremden Jurisprudenz zugrunde gehen.

3.4 Gesellschaftlicher Bereich: Weniger Netz und mehr Bewusstsein

In den vorausgegangenen Abschnitten hat sich gezeigt, dass der Cyberwar eine neuartige und komplexe Bedrohung für mehrere Ebenen der modernen westlichen Gesellschaften darstellt, für die bisher nur unzureichend Konzepte existieren, dieser zu begegnen. Mit Blick auf die Wahrnehmung dieses alle Bereiche der nationalen Sicherheit gefährdenden Phänomens zeigen sich zwei wesentliche Aspekte: Einerseits wird die Bedrohung aus dem Internet sowohl auf individueller als auch auf gesellschaftlicher Ebene völlig unterschätzt. Würden die deutschen Sicherheitsbehörden heute verkünden, chinesische Agenten wären verhaftet worden, weil sie auf frischer Tat ertappt wurden, wie sie Sprengsätze am Bundeskanzleramt, in Fabrikhallen von Airbus und in verschiedenen Kraftwerken und Stromverteilerkästen in ausgewählten deutschen Innenstädten befestigt hätten, wäre die BRD in heller Aufregung. Gleiches gilt wohl für jede andere westliche Gesellschaft, die sich mit derartigen Neuigkeiten konfrontiert sähe. Doch als etwa das Wall Street Journal 2009 verkündete, dass China logische Bomben, die sich weit verheerender auswirken können, in diversen amerikanischen Netzwerken platziert habe, blieben öffentliche Reaktionen weitgehend aus, obwohl das Platzieren logischer Bomben keinesfalls der Informationsbeschaffung dienen oder als Hintertür für ein System fungieren kann, sondern einzig und allein den Zweck hat, Schäden bei Hard- und Software anzurichten, was somit ausschließlich im Kontext von Kriegführung im Netz zu interpretieren ist.[80] Das Bewusstsein bei den Eliten wie auch innerhalb der Bevölkerung muss dringend für diese Art der ernsten Bedrohung geweckt werden, sodass auch die Bereitschaft entsteht, die notwendigen juristischen Schritte zu ermöglichen, um künftig die nationale Sicherheit zu verteidigen und zu bewahren. Derzeit ist dies nicht gewährleistet.

Der zweite Aspekt betrifft den Umstand, dass wie gezeigt völlige Sicherheit und Abwehr nicht möglich sind. Vor diesem Hintergrund ist das bisherige Modell der in allen Bereichen und weiter wachsendem Maße hochgradig vernetzten Gesellschaft zu überdenken. Da die einzige Sicherheit darin besteht, ein System vom Netz zu trennen, steht die Gesellschaft vor der Aufgabe, bestimmte mehr oder weniger zentrale Lebensbereiche umzugestalten und dabei zu »entnetzen«[81], was bedeutet dass die »Informatisierung sensibler und kritischer Systeme […] maximal reduziert werden [soll]. Verbindungen an große, externe Netze sollen restlos gekappt werden«.[82] Vorreiterstaaten des Cyberkrieges haben mit derartigen Schritten bereits begonnen. China hat sein nationales Netzwerk so ausgestaltet, dass der gesamte Internetverkehr über vier zentrale Portale läuft. Aus Sicht einer freiheitlichen Internetideologie, welche piratengleich undifferenziert und blindlings einem *anything goes* folgt, ein Graus, handelt es sich hierbei jedoch um eine

80 Vgl. ebd. S. 250 f.
81 Gaycken, Cyber Warfare, aaO. (FN 5), S. 206.
82 Ebd.

der wenigen Möglichkeiten, um Netzsicherheit wenigstens halbwegs zu gewährleisten, namentlich wenn sie intern noch in regionale Netzcluster unterteilt sind und Vorkehrungen getroffen wurden, kritische Infrastrukturen gleichsam auf Knopfdruck über sogenannte Kill Switches schnell und schadlos vom Netz zu nehmen. Denn die »Freiheit des Netzes ist […] eine nicht zu unterschätzende Teilursache des Cyberwar«[83]. Auch die USA haben mit ihrer *Trusted Internet Connection Initiative*, welche Teil der erwähnten CNCI ist, einen Weg der Entnetzung eingeschlagen; dort lautet die Vorgabe, die Verbindungen zwischen Regierungs- und öffentlichen Netzen auf 1,25% (!) der bisherigen Kapazität zu reduzieren.[84] Vor allem in dem mittlerweile de facto ausschließlich auf NCW basierendem Militärsektor wird eine Entnetzung schwierig und langwierig, sowohl aus technischen als auch aus den geschilderten ideologischen Gründen. Gleichwohl ist die sich abzeichnende Verzögerung problematisch weil aufgrund der bestehenden Schwäche vor allem im Defensivbereich in den kommenden Jahren erst einmal alle Tore für den Gegner offen stehen. Eine Entwicklung allerdings könnte die Bewusstmachung für die Netzproblematik schärfen: Nach der bisherigen weitgehend ungehemmten Verbreitung der Netztechnologien werden erste Nebenwirkungen wahrgenommen. Diese betreffen zwar eher Bereiche wie Cybermobbing oder Cybercrime, sind jedoch prinzipiell geeignet Eliten wie breitere Teile der Gesellschaft zusehends für die auch kriegsrelevanten Bereiche des Internets zu sensibilisieren. Entnetzung ist somit also auch weniger als Rückschritt, sondern als Fortschritt zu bewerten, sowohl im technischen als auch im normativen Sinne.

4. Quo vadis, Cybersociety?

Cyberkrieg zwischen nationaler Sicherheit und Freiheit

Damit allerdings bereits die Geburt einer Post-Informationsgesellschaft einläuten zu wollen erscheint an dieser Stelle noch übertrieben. Dass jedoch die Gesellschaft bereit sein muss, zur weitestgehend möglichen Wahrung des jetzigen Gesellschaftsmodells mit all seinen freiheitlichen Facetten ein höheres Regelungsmaß gerade auch im virtuellen Raum hinzunehmen, steht außer Frage. Denn die von Internetidologen propagierte Freiheit des Netzes, welche automatisch zu einer freiheitlichen und friedlichen Domäne führt, hat sich notwendigerweise als Chimäre erwiesen. Die Abwesenheit von Ordnung, Regeln und Kontrollen kann in der physischen wie auch der virtuellen *Realität* zu nichts anderem führen als zu einem hobbesianischen Naturzustand mit all seinen Wirkmechanismen, sodass auch im Netz einzig das Recht des Stärkeren gilt und jeder Akteur virtuell wie zunehmend auch in der physischen Welt zum Jäger und zugleich zum Gejagten des anderen wird. Die Konsequenzen hat die Geschichte anhand von reichlich Empirie immer wieder demonstriert, nicht zuletzt am real existierenden Staatszerfall in vielen Teilen der heutigen Welt mit verheerenden Folgen, insbesondere dem Fehlen von elementarsten existenziellen Sicherheiten. Die Frage um die es hier letztlich geht, nämlich das Bewahren

83 Ebd. S. 210.
84 Ebd. S. 208.

des eigenen Way of Life, der eigenen Identität als freiheitlich-demokratischer Rechts- und Verfassungsstaat westlicher Prägung mit Schwerpunkten in den tertiären und quartären ökonomischen Sektoren auch angesichts der skizzierten Bedrohungen durch Cyberkriegsführung lässt sich somit anhand der Auswahl zwischen zwei zur Verfügung stehenden Optionen beantworten: »Entweder wird der eigene Staat das Netz kontrollieren, die Unabhängigkeit […] von Wissen und Meinen sichern und das autonome […] Agieren der Wirtschaft. Oder andere Staaten werden seinen Unwillen zur Kontrolle für ihre eigenen Bemühungen um Steuerung ausnutzen. «[85] An der Fähigkeit, diese Entscheidung zu fällen, wird sich die Frage nach der Zukunft unserer Gesellschaft entscheiden, denn sie stellt nichts anderes dar als eine Antwort auf die Frage, ob unser eigenes Gesellschaftsmodell dies leisten kann oder sich letztlich doch der Autoritarismus sich als die überlegene Form des Cyberzeitalters erweisen wird. Eines ist klar: Der nächste Krieg wird auch im Netz geführt. Und bei ihm geht es um mehr als nur eine militärische Schlacht, es kann um alles oder nichts gehen. Ein Szenario, *nichts auf dem Radar* der Luftabwehr zu sehen ist ebenso Realität wie der Umstand, dass Cyberwar *nicht auf dem Radar* von Volk und Eliten zu finden ist. Gerade angesichts seiner Tragweite darf das Thema aber nicht länger von den Radarschirmen der Regierenden und der Öffentlichkeit verschwunden sein. Daher: Radar on, activate scan. Oder frei nach der alten römischen Kriegsweisheit: Si vis pacem, pare cyber-bellum.

Zusammenfassung

Der Beitrag befasst sich mit ausgewählten Herausforderungen, welche die neue Kriegsform Cyberwar, für die hochvernetzten westlichen Gesellschaften mit sich bringt. Es wird dargelegt, nach welchen Prinzipien Cyberkrieg funktioniert, in welchen Bereichen Verwundbarkeiten bestehen, welche Reaktionsmöglichkeiten existieren und welche Schwierigkeiten damit verbunden sind. Dabei wird verdeutlicht, dass Deutschland, wie andere westliche Gesellschaften, in vielfacher Hinsicht nur unzureichend auf die komplexen Herausforderungen des Cyberkrieges vorbereitet ist. Insbesondere die Parallelität der Diskurse Krieg und Internet, das mangelnde Bewusstsein von Bevölkerung und Eliten für den Grad der Gefährdung, die Defizite im nationalen wie im internationalen Recht, hier ein ideologisch fehlgeleiteter Liberalismusgedanke, dort ein derzeit kaum zu überwindendes neues Sicherheitsdilemma, und die Problematik, welche ein allzu sehr auf die Kräfte des Marktes vertrauendes Wirtschaftssystem mit sich bringt, werden im vorliegenden Beitrag als jene Herausforderungen betrachtet, mit deren Lösung die Antwort auf die Frage verbunden ist, ob die freiheitlich-demokratische Rechtsstaatsgesellschaft in der heutigen Form trotz der Cyberbedrohungen fortbestehen kann.

85 Gaycken, Cyber Warfare, aaO. (FN 5), S. 211.

Summary

This contribution deals with the challenges posed by cyber war, a new type of warfare, to the highly networked Western societies. It demonstrates the principles cyber warfare follows, shows in which areas vulnerabilities can be found, and explains which ways exist to react and what sort of difficulties come with these. It is made clear that Germany, as other Western societies, in many respects is only insufficiently prepared for the complex challenges of cyber warfare. In particular the parallelism of the two discourses on war on the one hand and the Internet on the other, the lack of consciousness on behalf of both population and elites, the deficiencies in national and international law, those being an ideologically misled idea of liberalism here and a currently hardly resolvable new security dilemma there, as well as the problems that accompany an economic system that counts too much on market forces, are regarded as those challenges the solution of which will provide the answer to the question whether the liberal-democratic society based on the rule of law will be able to sustain in their present form despite the threats from cyberspace.

Alexander Niedermeier, Not(hing) on the Radar. Cyber Warfare as Complex Challenge for the Highly Networked Society.