Scrum bietet eine offene Definition der Ziele (ein *wachsendes* Produkt) und eine dynamische Planung, Rollen, Formen der Teamarbeit, Prozesse und Ergebnisse. Die Partner im Forschungsprojekt bezeichnen Scrum als „ein offenes Verfahren, das dennoch Systematisierung und Orientierung bewerkstelligt" (S. 131). Porschen beschreibt die Methode und stellt sie auf den Prüfstand, was Akzeptanz und ethische Aspekte wie Entgrenzung, Selektion und Transparenz betrifft. Außerdem macht die Autorin Vorschläge zur Verbesserung, beispielsweise das Kooperationsmodell der Hospitationen, „in dem Beschäftigte andere Abteilungen und deren Arbeitsweisen, Problemstellungen und handelnde Personen näher kennen lernen können." (S. 137) In einem eigenen Abschnitt wird auch beschrieben, wie sich agile Entwicklungsansätze auf Hardware- Innovation übertragen lassen.

Förderer des Projekts *Künstlerisch, erfahrungsgeleitet, spielerisch – Management des Informellen zur Förderung innovativer Arbeit* (KES-MI): Bundesministerium für Bildung und Forschung, europäischer Sozialfonds für Deutschland

Ethisches: Entgrenzung, Selektion, Transparenz

„Die geschilderten Ansätze zu Selbstorganisation, Selbstverantwortung und Engagement sowie künstlerischen, erfahrungsgeleiteten und spielerischen Vorgehensweisen fördern Innovationsarbeit, sofern sie akzeptiert und praktiziert werden. Mit ihnen können aber auch Kehrseiten einhergehen: Sie können zu einer Extensivierung der Leistungen der Projektmitarbeiter und zu dadurch verursachten Überlastungen infolge von Leistungsverdichtung bzw. sogar zu Burn-out führen. Sie eröffnen zudem Möglichkeiten für Selektion und Kontrolle sowie eine direkte (erweiterte) Subjektkritik auf neuem Niveau. Die Ansätze können also einerseits zu Überlassungen des Gestaltungsprozesses an die Teambeteiligten dienen und die Einbindung und das Engagement der Mitglieder stärken. Sie führen andererseits aber auch zu einer neuen Transparenz für Projektmananger, Produktverantwortliche etc. und geben neue Kontroll- und Selektionsmöglichkeiten an die Hand." (S. 147)

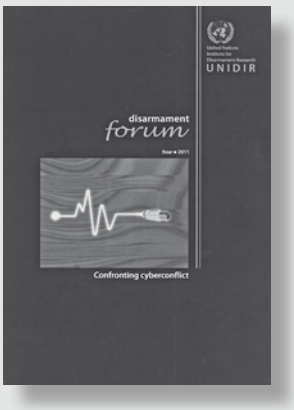
Dietrich Meyer-Ebrecht

Confronting Cyberconflict

UNIDIR Disarmament Forum 4/2011

"Cyberconflict is simply conflict carried out with the latest 'weapons' humanity has at hand", schreibt Kerstin Vignard, Herausgeberin der vierteljährlich erscheinenden Schriften des Disarmament Forum des United Nations Institute for Disarmament Research, im Editorial der Ausgabe 4/2011. In den Vordergrund der Konfliktszenarien, so führt sie weiter aus, ist das Thema dieses Heftes mittlerweile gerückt, weil ihm die sich immer fester etablierenden und weiter ausgreifenden digitalen Technologien und Infrastrukturen einen zunehmend fruchtbaren Nährboden bieten. Hinzu kommt die wachsende Zahl und Vielfalt potentieller Akteure, von staatlichen Instituten über ‚black hackers', Terrorgruppen, Kriminellen bis zu ahnungslosen Internetnutzern. Die Entwicklung eilt mit großen Schritten der ethischen, juristischen, politischen Debatte voraus, für eine Verständigung fehlt es nicht nur an verbindlichen Definitionen, sondern auch an grundlegendem Verständnis der komplexen Interdependenzen. In dieser Zeit, in der die internationale Gemeinschaft die Diskussion aufnimmt, will die vorliegende Ausgabe des Disarmament Forum mit fünf Aufsätzen zur Klärung der gesellschaftlich und politisch komplexen Thematik beitragen.

Mit „Cyberconflict and *jus in bello*" führt *Nils Melzer* in juristische Betrachtungen von kriegerischer Handlungen mit informatischen Mitteln ein. *Cyberwarefare* findet nicht in einem rechtsfreien Raum statt. Grundsätzlich gelten auch für die Anwendung von Cyberwaffen die etablierten Regeln und Prinzipien für kriegerische Handlungen. Das sind zum Einen die Allgemeinen Menschenrechte und im Speziellen das Internationale Humanitäre Völkerrrecht, die in den Genfer Konventionen festgeschriebenen humanitären Regeln für bewaffnete Auseinandersetzungen. Die Problematik liegt jedoch in der außerordentlich schwierigen Fassbarkeit, Erfassbarkeit und Bewertbarkeit von *cyber operations*. Weder findet eine physische Grenzüberschreitung statt, noch muss eine physikalische Wirkung – Zerstörung, Verletzung, Tod – die direkte und beabsichtigte Folge sein. Wohl aber können *cyber operations* konventionelle bewaffnete Konflikte auslösen. Insofern steht außer Frage, dass *cyber operations*, die diese Wirkung mittelbar haben, zu den Angriffshandlungen im konventionellen Sinne gerechnet werden müssen. Schwieriger wird es, wenn sie dazu dienen, lediglich strategische Objekte außer Funktion zu setzen und derart indirekt in Kampfhandlungen eingreifen. Eine spezielle Problematik stellt auch die Zuordnung der Akteure dar. Die Genfer Konventionen schützen Zivilpersonen. Zählt nun der IT-Spezialist in einer fernab vom Austragungsort eines bewaffneten Konflikts stationierten *cyber operation group* dazu, darf er Ziel eines – ggf. todbringenden



United Nations; Institut for Disarmament Research UNIDIR; http://www.unidir.org/bdd/fiche-periodique.php?ref_periodique=1020-7287-2011-4-en

– Gegenangriffs sein? Nicht in allen Fragen kann das derzeitige Rechtsverständnis extrapoliert werden. Es bedarf der internationalen politischen Diskussion und einer Verständigung über einen verbindlichen Codex für militärische *cyber operations*, bevor diese zu katastrophalen Situationen führen.

Brian Weeden stellt in seinem Beitrag „Cyber offence and defence as mutually exclusive national policy priorities" die ‚virtuelle Monokultur' im Cyberspace als ein neuartiges Problem der Militärtechnik heraus. Im Gegensatz zu konventionellen Waffensystemen, die proprietäre Entwicklungen der jeweiligen Rüstungsindustrie darstellen und deren Funktion und Innenleben nach Kräften geheim gehalten werden, bewegen sich *cyber operations* in einem universellen Medium, nutzen global die selben Hardware- und Softwarekerne. Daraus folgt eine ungewollte gegenseitige Transparenz bezüglich der für *cyber operations* verfügbaren Mittel, aber auch eine Symmetrie der Verletzlichkeit. Am Beispiel *Stuxnet* setzt der Autor die politische Brisanz auseinander, die die Nutzung ziviler Technologien, Produkte und Infrastrukturen für militärische Zwecke und – vice versa – die Proliferation militärischer Entwicklungen ins Zivile haben. Jede Entdeckung einer Sicherheitslücke bietet einen strategischen Vorteil – solange der Gegner sie nicht kennt … Zum Schaden der Zivilgesellschaft steht die Industrie folglich unter politischem Druck, strategisch nutzbare Sicherheitslücken nicht aufzudecken. Das in der Symmetrie liegende Junktim – verschaffe ich mir einen strategischen Vorteil oder schütze ich meine zivilen Systeme? – führt dazu, dass ein Staat, der auf Angriffsstärke setzt, sich im Gegenzug verletzlicher macht. Keine Lösung aus diesem Dilemma ist es, im Militär- und Sicherheitsbereich proprietäre Systeme einzusetzen. Diesen fehlt die evolutionäre ‚Reifung' in der Vielfalt der zivilen Anwendung, ohne die sich unvermeidliche Schwachstellen in der heutige hochkomplexen Hardware und Software nicht ausmerzen lassen. Wie man es dreht: Offensivkraft und Defensivstärke – beides ist unvereinbar! Hier eine gesellschaftsverträglich Balance zu finden, ist eine hohe Herausforderung an die Politik.

Statt Szenarien zu entwerfen, in denen sich Staaten in einen Wettlauf befinden, wer die neusten Sicherheitslücken entdeckt und diese am längsten geheim halten kann, plädiert *Ben Baseley-Waker* im folgenden Beitrag für „Transparency and confidence-building measures in cyberspace […]". Er befasst sich zunächst mit dem grundsätzlichen Problem der Grenzziehung und Attributierbarkeit*: Cybercrime – cyberespionage – cyberwarfare*, staatlicher Akt oder subversive Akteure? Die Grauzone birgt die Gefahr der Überreaktion und – in der Folge – Eskalation in sich, die Gefahr auch, dass Dritte in Haftung genommen werden, deren IT-Infrastrukturen missbräuchlich in Aktionen einbezogen werden. Erschwert wird die Situation durch unterschiedliche staatlich Perspektiven: Wird im *cyberspace* hier ein ‚Hort der Freiheit' gesehen, wird er anderswo als Bedrohung des Staates wahrgenommen. Von Nöten ist die Anwendung einer *cyber security diplomacy*, eine diplomatische Initiative zur zwischenstaatlichen Vertrauensbildung mit dem Ziel, den *cyberspace* transparenter, stabiler und vorhersehbarer zu machen. Mit diesem Ziel fand eine erste Konferenz, die *London Conference on Cyberspace*, im September 2011 statt. Russland und China brachten Vorschläge zur Selbstbeschränkung ein, gegen die jedoch die USA und Großbritannien opponierten. Einen anderen Ansatz versucht die *International Telecommunication Union* (ITU) mit ihrem Regelwerk. Die Ansätze sind ein Beginn. Es fehlt jedoch an Energie, sie voranzubringen. Angesichts der schnellen Entwicklung drängt der Autor zur unverzüglichen Fortsetzung der Initiativen „[…] towards norms of behaviour".

Diese Forderung nimmt *James Andrew Lewis* in seinem Beitrag „Confidence-building and international agreement in cybersecurity" auf. Auch Lewis geht von der Gefahr aus, dass bereits eine Fehlinterpretation einer *cyberaction* einen Krieg triggern kann. Begegnet werden muss dieser Gefahr mit internationalen Vereinbarungen. Angesichts der Schwierigkeit der Formulierung von Verträgen, die bereits bei den Definitionen beginnen, und der Problematik, geltende Gesetze auf den *cyberspace* auszudehnen oder umzudeuten, sieht er einen ersten Schritt darin, eine Codex für Verhaltensnormen aufzustellen. Im Sinne eines *norm-based approach* legte bereits in 2010 eine vom UN-Generalsekretariat zusammengerufene *Group of Governmental Experts* (GGE) in einem zweiten Anlauf einen knapp gehaltenen aber substanziellen Konsensbericht vor, der mit fünf grundlegenden Empfehlungen eine gute Grundlage für zukünftige Verhandlungen abzugeben verspricht. Zahlreich sind dennoch die Hindernisse auf diesem Weg. Belastend sind Geheimdienst- und Kalten-Kriegs-Allüren, die Tendenz zu einem Mehr an staatlicher Kontrolle. Schwer zu akzeptieren sind die Beschränkung von Spionagetätigkeit (wann ist der Einbruch in ein Computersystem ein Angriff?), der Rückzug von ‚grauen Märkten' (ironischerweise kommt gerade aus den Staaten, die sich vor Angriffen schützen möchten, die Technologie für diese), der Verzicht auf nichtstaatliche Akteure (‚*patriotic hackers*'). Immer noch ermuntert das Attributierungsproblem, die tatsächliche oder auch nur vermeintliche Schwierigkeit der Rückverfolgung und Zuordnung von *cyber operations* eher zu einer Intensivierung der Aufrüstung und Aktivität. Der Autor kommt zu der Schlussfolgerung, dass der Abschluss bindender multilateraler Verträge unter den gegebenen Umständen („Cyber attack is a behaviour rather than a technology"), aussichtslos ist. Er setzt statt dessen auf inkrementelle Fortschritte in der Hoffnung, dass die tiefe ökonomische Verflechtung insbesondere der Industriestaaten die Einigung auf internationale Standards in *cybersecurity* zwingend fordern werden.

Dass dies jedoch nicht nur die Industriestaaten angeht, thematisiert *John B. Sheldon* in „Achieving mutual comprehension: why cyberpower matters to both developed and developing countries". Entwicklungsländer sind zur Zeit an den beschriebenen Verständigungsprozessen kaum beteiligt. Diese Kluft kann gefährlich werden, denn der *cyberspace* kennt keine Territorialgrenzen, er hat Einewelt-Charakter. Sheldon fasst die Motivation für eine unumschränkte Verständigung in fünf Statements zusammen. (1) Durch seine nahezu unbegrenzte Reichweite verändert der *cyberspace* Gesellschaftsmechanismen und gewinnt auf diese Weise eine politische Wirkung, die auch in Entwicklungsländern zur Kenntnis genommen werden muss. (2) Industriestaaten besitzen quasi ein Monopol auf Technologie und Standards, für die Produktion (miss)brauchen sie jedoch die Entwicklungsländer; dort wiederum sind wichtige Zukunftsmärkte, und von dort kommen die Rohstoffe. (3) Die derzeitige Asymmetrie – kräftemäßig unterlegene Entwicklungsländer, ungleich verletzlichere Industriestaaten – könnte erstere zu *cyber attacks*, die nicht viel Aufwand erfordern, verleiten. (4) Die Verfolgung von Cyberkriminalität und Cyberterrorismus erfordert gemeinsa-

mes Handeln. (5) Selbst wenn keines dieser Argumente am Dialog uninteressierte politische Akteure überzeugt, müssen auch sie begreifen, „You may not be interested in cyberpower … but cyberpower is interested in you." Sein Facit: Die Kluft zu schließen, ist essentiell für eine weltpolitische Stabilität. Nicht nur militärisch relevante *cyberconflicts*, sondern alle Konflikte, die die Informationstechnologie mit ihrer unaufhaltsamen Durchdringung provoziert, müssen unverzüglich auf die politische Agenda gesetzt werden.

Die fünf Aufsätze dieses Heftes geben fakten- und facettenreiche Einblicke aus einer Reihe nichttechnischer Perspektiven, die für die geopolitische, geostrategische und gesellschaftliche Einschätzung der Thematik unverzichtbar sind. Für unsere ‚Mission', Brücken zu bauen zwischen Technik und Gesellschaft, technischen Einblick zu übersetzen in Impulse für die Friedensbewegung, vermitteln die sich in ihrer Sichtweise ergänzenden Beiträge wichtige Anregungen. Das Heft kann kostenfrei bezogen werden:

Stefan Hügel

Grundrechte-Report 2012

Der alternative Verfassungsschutzbericht

Wie jedes Jahr im Mai – zum Geburtstag des Grundgesetzes – stellten acht deutsche Bürgerrechtsorganisationen am 21. Mai 2012 der Öffentlichkeit in Karlsruhe den aktuellen Grundrechte-Report vor. Der als alternativer Verfassungsschutzbericht konzipierte Grundrechte-Report nennt aktuelle Missstände beim Namen. Er dokumentiert Verletzungen der verfassungsmäßig garantierten Grundrechte der Bürger und Bürgerinnen in Deutschland und erscheint mittlerweile im 16. Jahr. Der Grundrechte-Report 2012 befasst sich unter anderem mit Spitzeltätigkeiten des Staates, der Einschränkung der Demonstrationsfreiheit, der Verschärfung des Ausländer- und Flüchtlingsrechts, der Diskriminierung von Behinderten und der Entrechtung von Alten und Pflegebedürftigen.

„‚Sicherheit durch Recht und Ordnung' war 1969 der (seinerzeit durchaus beargwöhnte) Slogan der NPD zur damaligen Bundestagswahl", so die Herausgeber in der Einleitung. „Könnte dieser Slogan nicht inzwischen als Einheitslosung der herrschenden Politik gelten? Freiheitsrechte kommen nur noch in Sonntagsreden und als politischer Luxusartikel vor … es ist eigentlich nur noch die Frage, wie man die Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs für Menschenrechte umgehen oder ‚austricksen' kann, um eine Sicherheit vorzutäuschen, die es in Wirklichkeit so nicht gibt."

Ein Schwerpunkt des aktuellen Berichts ist die Freiheit im Netz und das Recht auf informationelle Selbstbestimmung. So befasst sich der Report mit den neuen Herausforderungen sozialer Netze wie Facebook & Co. an das Datenschutzrecht, mit der außer Kontrolle geratenen Überwachung mit dem Staatstrojaner, mit mangelndem Datenschutz im Strafvollzug, Videoüberwachung, der elektronischen Gesundheitskarte und Funkzellenabfragen als neuer Bedrohung der Versammlungsfreiheit.

Aber auch Bedrohung der Freiheit des Glaubens – durch das Privileg der Staatskirchenleistungen an die christlichen Kirchen –, die Bedrohung der Meinungsfreiheit – durch die Bestätigung einer Fristlosen Kündigung wegen Whistleblowing durch deutsche Arbeitsgerichte, die zu einer Verurteilung der Bundesrepublik Deutschland durch den Europäischen Gerichtshof für Menschenrechte geführt hat – und die Bedrohung des Engagements gegen Faschismus – durch die vom Bundesministerium für Familie, Senioren, Frauen und Jugend geforderte „Demokratieerklärung" – sind Thema des Bandes.

Grundrechte-Report 2012 – Zur Lage der Bürger- und Menschenrechte in Deutschland; Herausgeber: T. Müller-Heidelberg, E. Steven, M. Pelzer, M. Heiming, H. Fechner, R. Gössner, U. Engelfried und M. Küster; Preis 10,99 €; 234 Seiten; ISBN 978-3-596-19422-3; Fischer Taschenbuch Verlag; Juni 2012

Als Fazit bleibt: Wenn man sich mit der Situation der Bürgerrechte in Deutschland auseinander setzen will, ist der Band Pflichtlektüre.

Der diesjährige Bericht wurde von der früheren Bundesjustizministerin Prof. Dr. Herta Däubler-Gmelin vorgestellt. Er wird herausgegeben von der Humanistischen Union – vereinigt mit der Gustav-Heinemann-Initiative, dem Komitee für Grundrechte und Demokratie, dem Bundesarbeitskreis Kritischer Juragruppen, Pro Asyl, dem Republikanischen Anwältinnen- und Anwälteverein, der Vereinigung Demokratischer Juristinnen und Juristen, der Internationalen Liga für Menschenrechte und der Neuen Richtervereinigung.