Dietrich Meyer-Ebrecht, Ingo Ruhmann, Thomas Reinhold

Cyberwar & Cyberpeace: Sind neue Regeln im Cyberspace möglich?

Internationaler Pugwash-Workshop, Berlin, 23.–24. Oktober 2015

Militärische Aktivitäten können heute wohl nirgendwo mehr auf dieser Welt unbeobachtet ablaufen – außer im Cyberspace. Das klingt paradox, dient doch der Cyberspace als übermächtiges Instrument für eine Ausspähung bis in den letzten Winkel der Erde. Dennoch, mit den nötigen Kenntnissen und Mitteln ausgestattet, können zumindest Inseln im Informationsraum weitgehend vor Beobachtung geschützt werden. Hier können Waffen entwickelt, produziert und ‚stationiert' werden, ohne physikalischen Raum zu benötigen, hier können Waffen getestet und zum Einsatz vorbereitet werden, ohne physikalische Spuren zu hinterlassen, und ihre digitalen Spuren können verschleiert oder sogar ausgelöscht werden. Mit seinem überlegenen Potenzial zur Geheimhaltung ist der Cyberspace bereits seit Langem als fünfter Operationsraum – neben Land, Luft, See und Weltraum – in die militärischen Strategien fest eingebunden. In der Zivilgesellschaft sind Kenntnisse über militärische Aktivitäten im Cyberspace jedoch eher vage, auch nach den Snowdenschen Enthüllungen. Das ist nicht nur der Geheimhaltung zuzurechnen. Die abstrakte Natur der Materie bringt es mit sich, dass ein öffentliches Interesse wenig ausgeprägt ist. Entsprechend schwierig ist es auch, die Auswirkungen militärischer Cyberoperationen abzuschätzen. Unklar ist zudem die völkerrechtliche Einschätzung. Über reale Risiken hinaus ist es die Summe dieser Unsicherheiten, die bedrohlich wirkt.

Vor dieser Situation ist es umso wichtiger, dass das Thema *Cyberwar* zunehmend von wissenschaftlichen Veranstaltungen aufgegriffen wird, so auch vom diesjährigen Treffen der Deutschen *Pugwash*-Gruppe in Berlin. Die deutsche Pugwash-Gruppe wurde im Zusammenhang mit der Gründung der *Vereinigung Deutscher Wissenschaftler* (VDW) bereits im Jahre 1959 ins Leben gerufen, zwei Jahre nach der ersten *Pugwash Conference on Science and World Affairs*. Mit dem diesjährigen Workshop *Cyberwar & Cyberpeace: Sind neue Regeln im Cyberspace möglich?* setzt die Gruppe eine Veranstaltungsreihe zu Cyberthemen fort, die im Rahmen der europäischen Pugwash-Gruppen im Sommer 2013 in den Niederlanden initiiert wurde. Ziel des Workshops war es, die mit der Thematik befassten nationalen und internationalen Gemeinschaften von Wissenschaft, Politik und Zivilgesellschaft miteinander ins Gespräch zu bringen und einen Beitrag dazu zu leisten, dass sowohl in Fachkreisen als auch in der Öffentlichkeit ein Bewusstsein für die Komplexität der Sachzusammenhänge entsteht.

Das Programm spiegelt die Vielfalt der Thematik wider. Eröffnet wurde es mit Vorträgen über die technischen Aspekten gegenwärtiger Cyberangriffe, über Konsequenzen für die globale digitale Infrastruktur und über Möglichkeiten für Gegenmaßnahmen und Verteidigung. Hier wurde auch speziell nach den Aufgaben der Regierungen und der Rolle der EU gefragt. Dass der Cyberspace als neuer politischer Raum verstanden werden muss, dessen Gestaltung neue juristische und friedenspolitische Fragen aufwirft, machten Vorträge zur juristischen Situation deutlich, die sich mit der Anwendbarkeit internationalen Rechts im Cyberspace, mit der Bedeutung des Tallinn-Manuals in dieser Hinsicht und mit der Herausforderung der NSA-Affäre an nationales und internationales Recht befassten. In zwei Vorträgen wurde analysiert, wie effektiv internationale Bemühungen zur Gewährleistung der Sicherheit in den globalen digitalen Netzen sein können. Eine Panelsitzung befasste sich mit den Forderungen an Verwaltung, Politik und Wirtschaft, speziell bezüglich der Sicherheitsbelange, und dies auch im Hinblick auf humanitäre Fragen.

Einen der für Cyberangriffe spezifischen Aspekte waren die Folgen der Schwierigkeiten einer Attribution. Dass die Herkunft von Angriffen und die Identifikation eines Angreifers ein Problem ist, hat auf politischer und strategischer Ebene die Folge, dass es ohne klare Attribution auch keinen eindeutigen Gegner gibt und damit auch keine politische Möglichkeit der Abschreckung oder Begrenzung. Aus Sicht der Diplomatie gibt es damit keine Möglichkeit zwischenstaatlicher Abkommen, sondern allein die Option auf eine weitere Aufrüstung.

In der Plenarsession *Military Options and Arms Control für the Cybersphere* wurden systematisch die für bisherige Rüstungskontroll-Vereinbarungen entwickelten Denkweisen, Ziele und Umsetzungsmaßnahmen betrachtet und versucht, diese auf den Cyberspace zu übertragen. Diese Sichtweise erlaubt neue Schlussfolgerungen für die Arbeit zur Begrenzung der Rüstung im Cyberspace. So ist die bei Atomwaffen – etwa durch den Verzicht auf Abwehrraketen – mögliche Option auf Nicht-Verteidigungsfähigkeit in der Informatik keine Option, da IT-Sicherheit (die vielfach ohnehin lückenhaft ist) gegen vielerlei Gefährdungen erreicht werden muss. Dagegen kann eine Strategie der gegenseitigen Zerstörung (*mutually assured destruction*, MAD, bei Atomwaffen von Bedeutung) bei Cyberangriffen durchaus eine Option sein, wenn demonstriert werden kann, dass ein Gegenschlag auch bei und nach einem Angriff erfolgen kann. Allerdings liegt auch hierin eher eine Tendenz zur Aufrüstung. Ein beachtenswerter Sonderfall war der einer unilateralen reziproken Abrüstung wie beim Zerfall der UdSSR: USA und UdSSR haben ihre Atomwaffen einseitig ohne Vereinbarung zurückgezogen, um zu einer schnellen Lösung zu kommen. Als universeller Weg zur Rüstungskontrolle wurde der Aufbau vertrauensbildender Maßnahmen beschrieben, die in der IT-Welt etwa die verstärkte Kooperation von CERTs bedeuten würde. Etablierte Strategien zur Abrüstung sind in jedem Fall wichtige und viel zu wenig untersuchte Ansatzpunkte auch für die Abrüstung im Cyberspace.

In dieser Session ging es auch darum, für die Rüstungskontrolle aus den Erkenntnissen zu lernen, die aus den Snowden-Dokumenten zu ziehen sind. Dies fängt damit an, dass Cyberwaffen bisher gar nicht als solche erkannt werden. Die XKeyscore-Software der NSA ist eine klassische Angriffswaffe, über die lediglich als Spionagewerkzeug berichtet wird. Auch die Infrastrukturen der Cyberkrieger sind heute noch nicht ausreichend erhoben und systematisiert. Wie das *Transgression*-Programm der NSA zeigt, haben die Cyber-Einheiten genügend Kenntnisse voneinander, um sich gegenseitig – sogar auf dritter und vierter Ebene – durch Cyberattacken die Ergebnisse der jeweils gegnerischen

Arbeit zu stehlen. Diese Erkenntnisse ließen sich ebenfalls für die Rüstungskontrolle nutzen. Mindestens ebenso wichtig sind die personellen und finanziellen Ressourcen der Cyber-Einheiten, die – der Darstellung verfügbarer Daten zufolge – das sechs- bis zehnfache der Ressourcen zur Verfügung haben wie ihre Gegenüber in der zivilen Strafverfolgung und der zivilen staatlich organisierten IT-Sicherheit. Auch diese Kräfteverhältnisse sollten für die Rüstungskontrolle bewertet und genutzt werden. Als Fazit wurde gezeigt, dass die zahlreichen neuen, aber auch die bereits bekannten Daten und Fakten zu Cyberwar-Akteuren bei weitem nicht angemessen für Rüstungskontrollansätze genutzt werden und damit zahlreiche Lösungsansätze ungenutzt bleiben.

Ein wichtiges Element der Pugwash-Workshops ist die Diskussion spezieller Themen in Arbeitsgruppensitzungen, die der persönlichen, thematischen und wissenschaftlichen Vernetzung dienen sollen. In parallelen Sitzungen waren drei Arbeitsgruppen angesetzt. Es ging darin um die Kontrolle des Internet (*Internet Governance*) und den Datenschutz, um die Verwundbarkeit der zivilen kritischen Infrastrukturen wie der Energieversorgung oder des Finanzsystems (*Humanitarian Issues*) und um die Frage, ob der Cyberspace zur Arena einer neuen Kriegsführung werden könnte oder dies bereits ist (*Cyberspace and Warfare*).

Diese letztgenannte Arbeitsgruppe fokussierte sich in ihrer Diskussion auf das friedenspolitisch zentrale Problem der Rüstungskontrolle: Lassen sich Methoden der Rüstungskontrolle, die in den vergangenen Jahrzehnten für andere Waffentechnologien entwickelt wurden, auf den Cyberspace übertragen? Eine entscheidende Voraussetzung dafür wurde in einer präziseren Fassung des Begriffs ‚Cyberwaffe' gesehen, insbesondere um eine Abgrenzung zu legitimen zivilen sowie defensiven militärischen Anwendungen wie Penetrationstests zu gewährleisten. Eine Klassifikation über das Schadenspotential erscheint notwendig, aber schwierig. Es fehlen verlässliche Klassifikationsmethoden. Vor allem lassen sich Kettenreaktionen beim Angriff auf IT-Systeme nicht abschätzen. Weitere wissenschaftliche Arbeit ist dringend geboten, insbesondere um eine Grundlage für internationale Vereinbarungen zu legen.

An dieser Arbeitsgruppe nahm ein einziger Informatiker teil. Überhaupt waren Informatiker.innen deutlich unterrepräsentiert, nimmt man den Ruf nach wirkungsvollerer technisch-wissenschaftlicher Unterstützung friedenssichernder Ansätze angesichts des Potenzials militärischer Operationen im Cyberspace ernst. In Gesprächen am Rande wurde eine zögerliche Haltung der Informatik – hier speziell im Fachgebiet Cybersecurity – deutlich, sich mit diesem ‚heißen' Themenkomplex zu befassen. Dabei ist eine aktive Teilhabe der Disziplin auch deshalb so wichtig, als der Cyberspace im Gegensatz zu allen anderen militärischen Operationsräumen ausschließlich von Menschen gemacht ist und seine Funktionsweise von Fachleuten definiert und kontrolliert wird. Beeindruckend war andererseits, welche Vielfalt an wissenschaftlichen Disziplinen an diesem Workshop beteiligt war. Die Komplexität des Themas fordert dies. Allerdings, und das ist eine andere Beobachtung, müssen die Verständigungsbrücken zwischen den Wissenschaften noch erheblich ausgebaut werden.

Die Präsentationen zu einzelnen Vorträgen sowie Berichte aus den Arbeitsgruppen sind aus dem Internet abrufbar: *http://neu.vdw-ev.de/veranstaltungen/international-pugwash-workshop/*

Übernommen mit freundlicher Genehmigung aus *Wissenschaft und Frieden* 1/2016.

FIfF e.V. – Pressemitteilung

FIfF fordert endlich Aufklärung zum Cyberangriff auf den deutschen Bundestag

25. August 2015 – Im Mai wurde bekannt, dass zahlreiche Computer im *Parlakom*-Netzwerk des Deutschen Bundestages Schadsoftware enthalten. Diese ermöglicht es unbekannten Angreifern, Daten von Abgeordneten und ihren Mitarbeiter.innen zu entwenden. Nach wie vor gibt es bisher keine öffentlichen Informationen und es existieren lediglich Hinweise, dass mehrere Gigabyte E-Mail-Schriftverkehr von Parlamentariern und ihren Mitarbeitern kopiert wurden. Da[illegible] Informationen über deren Pläne dabei nur erahnen. Einzelne Abge[illegible]ne Institution hingegen, die klar 2014 über mögliche Manipulatio[illegible]e und ihrer Werte auf dem Gebiet dennoch wurde das Parlakom-Sy[illegible] muss unabhängig sein. Im Fall abgeschaltet. Angesichts der Bedeutung des Systems als primäre Kommunikations- und Arbeitsplattform des deutschen Bundestages kritisiert das FIfF, dass zuständige Stellen den Angriff offenbar nur zögerlich und mangelhaft untersucht haben. Die Öffentlichkeit wurde bis jetzt nur unzureichend über den Schaden und die Konsequenzen für die Arbeit der Volksvertreter informiert.

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Fatal ist, dass nicht nur die Parlamentarier hilflos erscheinen, sondern auch die Behörden, deren Aufgabe es ist, den Angriff zu untersuchen. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI), das für den Schutz von Bundeseinrichtungen vor Internetangriffen verantwortlich ist, gibt es nach wie vor keine offizielle Stellungnahme. Dabei muss die Rolle des BSI, das direkt dem Innenministerium unterstellt ist, selbst kritisch hinterfragt werden. Als Teil der Regierung, deren Handeln eigentlich von den Parlamentariern kontrolliert werden soll, könnte das Ministerium durch die Untersuchung der Rechner aller Par[illegible] des BSI sind Zweifel darin berechtigt, zumal die Behörde immer wieder auch im Verdacht der Kooperation mit dem US-amerikanischen Geheimdienst NSA stand.

„Insider" und Medien spekulieren währenddessen über den Ursprung des Angriffs. „Ein sinnvoller Rückschluss auf einen bestimmten Angreifer ist jedoch kaum gesichert möglich. Im Bereich mutmaßlich zwischenstaatlicher Spionage sind derartige Fragen ohnehin vielmehr Gegenstand außenpolitischer Interessen als echter Fakten", stellt Thomas Reinhold klar, Campaigner