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 Arb
persönlichen, thematischen und
dienen sollen. In parallelen Sitzu
pen angesetzt. Es ging darin um d
net 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
ißen' Themenkomplex zu befas-
habe der Disziplin auch deshalb
im Gegensatz zu allen anderen
n 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.

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

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. Das Ausmaß der Affäre lässt sich dabei nur erahnen. Einzelne Abgeordnete wurden bereits im Juni 2014 über mögliche Manipulationen ihrer Computer informiert; dennoch wurde das Parlakom-System erst jetzt für Reparaturen 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.

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 Parlamentsmitglieder mittelbar an Informationen über deren Pläne und Standpunkte gelangen. Eine Institution hingegen, die klar dem Schutz unserer Demokratie und ihrer Werte auf dem Gebiet der Informationstechnik dient, muss unabhängig sein. Im Fall des BSI sind Zweifel daran 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

der Cyberpeace-Kampagne des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF). „Es ist ebenso vorstellbar, dass die scheinbaren Quellen des Angriffs durch Dritte benutzt wurden, um absichtlich Spuren in eine falsche Richtung zu legen." Dies gilt umso mehr, da die Rechner, von denen der vermeintliche Angriff erfolgte, zum Zeitpunkt der Angriffe selbst fehlerhafte Software in Form der *Heartbleed*-Schwachstelle enthielten. Dies ergab die Analyse eines unabhängigen IT-Experten im Auftrag der Bundestagsfraktion der Partei *Die Linke*. Nicht russische – wie zwischenzeitlich gemutmaßt wurde – sondern beliebige Geheimdienste könnten am Ende hinter diesem Angriff stecken.

Immer wieder gelingt es Angreifern, sich Zugang zu sensiblen oder kritischen IT-Strukturen zu verschaffen.

„Computer sind grundsätzlich angreifbar, wir müssen unsere Systeme daher besser schützen und die Sicherung von IT angesichts deren zentraler gesellschaftlichen Bedeutung als Kernaufgabe verstehen", mahnt Stefan Hügel, Sprecher der Cyberpeace-Kampagne und Vorsitzender des FIfF e.V. Dazu bedarf es vor allem auch seitens der Bundesregierung ein klares Bekenntnis zur Förderung sicherer Informationstechnik, des Schutzes von IT-Strukturen durch öffentliche und unabhängige Institutionen und die Abkehr von nebulösen Geheimdienstkooperationen. Vor allem aber brauchen wir einen transparenten und einer Demokratie würdigen Umgang mit derart massiven Vorfällen wie dem Bundestagshack – einem Cyberangriff auf die Infrastruktur der Vertretung der gesamten deutschen Bevölkerung.

Sylvia Johnigk – Rede bei der Demonstration

Freiheit statt Angst – Kundgebung 10. Oktober 2015, München

Ich werde einen Aspekt in den Fokus rücken, der in der Diskussion zu wenig beachtet wird – die militärische Motivation für Überwachung.

Was treibt unsere Regierungen an, sich seit Jahrzehnten beim Versuch, die Voratsdatenspeicherung zu etablieren, ständig bei unseren Verfassungsgerichten blutige Nasen zu holen?

Parallel terrorisieren uns Regierung und Sicherheitsbehörden seit Jahren mit abstrakten Gefahren und vermeintlichen Terrordrohungen, um uns weichzukochen. Damit wir endlich folgsam werden – sie wollen, dass wir zukünftige Überwachungsmaßnahmen klaglos akzeptieren: an Flughäfen, Bahnhöfen, Autobahnen, in Bahnen, Bussen, Stadien, auf öffentlichen, nicht-öffentlichen Plätzen und inzwischen, weil es so schön einfach geht, im digitalen Raum.

Dabei geht es ihnen um uns alle zusammen – die Gesellschaft als Ganzes, die, wenn sie allumfassend überwacht wird, leichter manipulierbar und beherrschbar ist.

Je mehr die Regierung über die Stimmung in der Gesellschaft weiß und mit welchen Faktoren sie sich verändert, desto leichter fällt es, die Stimmung durch gezielte Manipulation zu beeinflussen.

Es geht in erster Linie darum, hegemonale wirtschaftliche Strukturen zu festigen, uns gefügig für TTIP, Ceta, Hartz IV, private Vorsorge zu machen und um Kriege zu führen – jetzt auch im digitalen Raum.

Das Strategiepapier der Verteidigungsministerin von der Leyen sieht vor, im digitalen Raum, beim Cyberkrieg, aktiv mitzuwirken – deshalb muss die Bundeswehr digitale Waffen für einen Angriffskrieg bauen.

Interessanterweise spielt bei Kriegen Überwachung und Spionage – und damit die Vorratsdatenspeicherung – eine tragende Rolle.

Überwachung im eigenen Land bedeutet die eigene Gesellschaft, Spionage bedeutet den Gegner zu kennen. Dabei geht es nicht nur um technische sondern insbesondere auch um organisatorische und gesellschaftliche Informationen, die genutzt werden – um Kriege mit möglichst großer Zustimmung in der eigenen Bevölkerung führen zu können.

Das eigentlich kriegsmüde, pazifistische Deutschland soll wenigstens den digitalen Krieg mittragen. Aber digitale Kriege bleiben nicht digital, sie haben wie herkömmliche Kriege Auswirkungen auf Menschen.

Im digitalen Krieg werden Stromnetz und Telekommunikationseinrichtungen angegriffen. Um digitale Waffen bauen zu können, muss man Schwachstellen in Computern geheimhalten und kann die Computer der eigenen Bevölkerung nicht mehr dagegen absichern.

Wir haben als FIfF deshalb eine Kampagne für Cyberpeace gestartet, die sich insbesondere gegen Cyberwaffen richtet. Unterschriftenlisten liegen an unserem Stand aus.

Ich will grundsätzlich nicht überwacht werden, und schon gar nicht um mich manipulieren zu lassen, ich bin keine Marionette sondern ein freier Mensch, ich bin Informatikerin und ich warne vor einem digitalen Krieg, der erst durch Überwachung möglich wird.

Münchner FIfF-Aktivisten im Einsatz

Foto: Sylvia Johnigk