überhaupt mit dem Prinzip des Geheimen kompatibel sind, von unfreier/closed-source Software über Geschäftsgeheimnisse bis hin zu Geheimdiensten). Ich denke, die Antwort lautet sowohl aktuell betrachtet als auch histori

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

Anmerkungen

1 T. Schwarze und A. Gruber, Darf der BND das?, http://www.zeit.de/politik/deutschland/2013-08/bnd-nsadatenweitergabegesetz/komplettansicht, 5. August 2013.

2 BVerfG, 1 BvR 370/07, https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, 27.2.2008.

3 In einer Rede vor dem Bundesverfassungsgericht als Sachverständiger uhe, 10.10.2007.

rvat.unibe.ch/dfr/bv088203.html,

Deutschland: Post- und Telefonüberwachung in der alten Bundesrepublik, 2013.

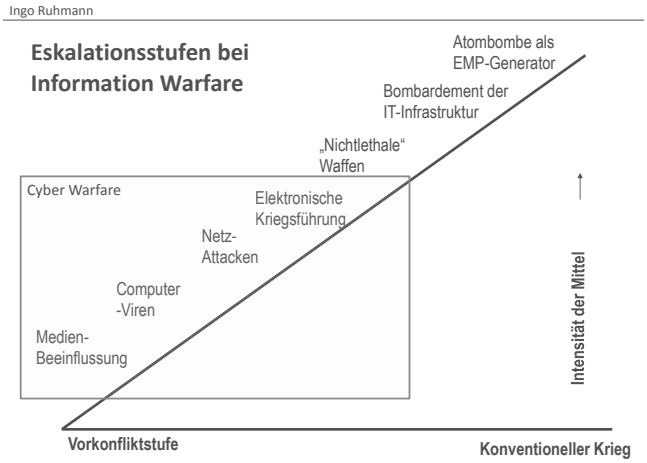
6 Koalitionsvertrag zwischen CDU, CSU und SPD , 18. Legislaturperiode, S. 148, 2013.

Ute Bernhardt, Ingo Ruhmann

Mitten im Cyberkrieg – Angriff auf die Zivilgesellschaft

Der seit dem Frühjahr 2013 weiter andauernde NSA-Skandal macht den Stellenwert staatlicher Hacker heute deutlich. Die bekannt gewordenen Dokumente lassen als Schluss nur zu, dass kein anderer als die NSA die leistungsfähigste und finanzstärkste Hackertruppe der Welt darstellt. Seit den 70er Jahren führt sie immer intensiver Cyberkrieg *gegen Freund und Feind. Nicht allein unsere Privatsphäre ist in Gefahr, sondern die gesamte Infrastruktur, die sichere IT-Systemen voraussetzt. Die Zivilgesellschaft, die das Internet zu ihrem Nervensystem gemacht hat, muss sich den Konsequenzen dieser Entwicklung stellen und staatlicher Computerspionage und -sabotage Einhalt gebieten. Wie dies möglich ist, war Thema der Arbeitsgruppe* Mitten im Cyberkrieg *auf der FIfF-Jahrestagung 2013.*

Zu Beginn des Workshops stellte *Ingo Ruhmann* eine Aufarbeitung der vom FIfF seit fast 30 Jahren bearbeiteten militärisch-geheimdienstlichen Überwachungsaktivitäten vor, die durch die beeindruckende Sammlung der mit Hilfe von Edward Snowden veröffentlichten Dokumente umfassend ergänzt und wesentlich konkreter fassbar wurden. Ausführlich ist dies auch in dem dieser Ausgabe beigelegten Dossier *Information Warfare und Informationsgesellschaft* (*Wissenschaft & Frieden*, Dossier Nr. 74) nachzulesen. Der erste Vortrag konzentrierte sich aber nicht auf Fragen der Überwachung, sondern der IT-Sicherheit. Dargestellt wurde, in welcher Weise Information Warfare und Cyberkrieg den Rahmen bilden für die Aktivitäten der amerikanischen und britischen Geheimdienste, die sich in jede Art von Kommunikation eingeklinkt haben.



Kommunikationsüberwachung war seit dem 19. Jahrhundert Aufgabe von Polizei und später Nachrichtendiensten. In allen Staaten ist gesetzlich geregelt, welche Unterstützung die Netzbetreiber für diese Überwachung leisten müssen. Neu an den NSA-Aktivitäten ist jedoch, dass die NSA seit den 1980er Jahren mit Cyber-Angriffswerkzeugen experimentiert hat – wozu interessante Presseberichte aus der Zeit von 1982 bis 2009 zu sehen waren –, und heute mit automatisierten Angriffswerkzeugen Trojaner und andere Schadsoftware auf IT-Systemen ihrer Opfer installiert. Wo diese Mittel nicht ausreichen, arbeitet seit Ende der 1990er Jahre eine spezielle Hackergruppe an gezielt durchgeführten Angriffen.

Die aufgrund der Medienberichte der NSA zuzurechnenden Trojaner wurden in einem Ausmaß nachgewiesen, das vergleichbar ist mit der am weitesten verbreiteten Schadsoftware, die konventionellen *Cyber-Kriminellen* zugeschrieben wird. Die Aufwände der NSA für das Aushebeln von Schutzmechanismen, von Verschlüsselungswerkzeugen und zur Sammlung von Kommunikationsdaten ist allerdings mit keinem anderen Akteur weltweit vergleichbar: Mit ca. 12 Mrd. US-Dollar pro Jahr ist die NSA zweifellos die mit den umfangreichsten Ressourcen ausgestattete Hackertruppe der Welt. Dass sich die NSA gegen Verbündete ebenso wie vermutete Gegner wendet, ist mittlerweile medial ausgiebig berichtet worden. Nach eigener Definition führen also die USA uneingeschränkten Cyberkrieg gegen Freund und Feind.

Fazit dieser Einführung war, dass die NSA wesentliche IT-Sicherheitsmittel umfassend kompromittiert hat. Gewissheit über die Zuverlässigkeit von IT-Sicherheitswerkzeugen kann es derzeit nicht geben. In einem *Cyberwar unter Freunden* kann Datenschutz daher nur ein Teil der Debatte sein. Sicherheit in der IT-Welt muss heute neu bewertet, viele lieb gewonnene Abläufe müssen mit neuen Sicherheitsmechanismen neu gestaltet werden. Dies, so das Ergebnis der Diskussion im Anschluss, ist ebenso Aufgabe für kritische IT-Experten unter anderem aus dem FIfF wie auch der Wirtschaft.

In seinem anschließenden Vortrag, der in diesem Heft in einem eigenen Beitrag dargestellt ist, konzentrierte sich der ehemalige MdB *Paul Schäfer* auf die sicherheitspolitische Rolle der Bundeswehr und deren Interessen an Aufklärungstechnik und -inhalten.

Die Auslandseinsätze vor allem in Afghanistan machen die Truppe abhängig von Aufklärungsdaten, die zumeist von anderen Alliierten gesammelt werden, da die eigenen Mittel begrenzt sind. Das Debakel um die Beschaffung von Überwachungsdrohnen, für die es zwar keine Flugzulassung gibt, aber eine ausgereifte Überwachungssensorik, die nun anderweitig genutzt werden soll, wird in Gänze nur im Zusammenhang mit früheren Beschaffungszielen und neuen Aufgaben nachvollziehbar. Auch die Aufgaben der im *Kommando Strategische Aufklärung (KSA)* zusammengezogenen Bundeswehr-Truppenteile für die elektronische, psychologische und die Cyber-Kriegsführung lassen einerseits erwarten, dass zusätzliche Aufgaben den Bedarf an neuer Technik nach sich ziehen werden. Andererseits sind die bestehenden Fähigkeiten nur äußerst schwer zu bewerten. Diese nur durch die besonderen Möglichkeiten eines Parlamentariers zu gewinnenden Einblicke leiteten über zu der Frage, welche Handlungsoptionen auch auf politischer Ebene aussichtsreich sein können.

Zur Systematisierung der Diskussion differenzierte *Ute Bernhardt* die Reaktionsmöglichkeiten und die potentiellen Akteure. Klar ist: Unbeobachtete Telekommunikation ist *das* strategische Grundrecht des Internet-Zeitalters. Vom Schutz einer einzigen Technik und einer einzigen Grundrechtsvorschrift hängen prinzipiell alle Aktivitäten im Internetzeitalter ab. Wenn alle Äußerungen und Aktivitäten durch Überwachung sichtbar werden, sind politische Willens- und Meinungsbildung, Entfaltung der Persönlichkeit, politische Teilhabe, Handlungsfreiheit unmöglich, sind Demokratie und Rechtsstaat verloren.

Allerdings geht es eben nicht allein um Überwachung. Ausgehend von den von NATO-Juristen gewählten Definitionen eines Cyberkrieges und deren Klassifikation von möglichen Angriffsformen im *Tallinn-Manual*[1] und den bekannten Fakten zum NSA-Skandal sind die Aktionen von NSA und GCHQ nach internationalem Recht als Cyberangriff zu werten. Ob es klug ist, diesen wiederum militärisch zu beantworten, darf bezweifelt werden. Allerdings ließe sich eine solche Attacke als Spionage und Sabotage oder staatlicher Cyber-Terrorismus begreifen. Dafür zuständig sind nun keine Datenschützer, sondern Strafverfolger. Nicht umsonst gibt es im Strafrecht Straftatbestände wie Computerspionage und Computersabotage. Das ist kein Novum: Auch im Kalten Krieg wurde mit der Staatsanwaltschaft gegen Großmächte und deren Spionageapparate vorgegangen.

Die Zurückhaltung der staatlichen Seite, hier tätig zu werden, macht allerdings andere Ansätze nötig. Die großflächige Kompromittierung der IT-Sicherheit zwingt die Wirtschaft dazu, technische und organisatorische Maßnahmen zu treffen, um IT und Geschäftsprozesse sicher und zuverlässig zu gestalten. Um interne und kundenbezogene Prozesse sicherer zu machen, müssen die Unternehmen kompromittierte IT ersetzen durch neue Kryptoverfahren und andere sichere IT-Lösungen. Erhebliche Entwicklungsaufgaben sind zu leisten, die Ressourcen binden und einen erheblichen Kostenfaktor darstellen werden. Der Aufwand dürfte ähnlich groß sein wie der beim Jahr-2000-Problem.

Hinzu kommen muss der klassische politische Protest, der aus Medienarbeit, der Arbeit von NGOs und deren Beratung des politischen Raumes, der Medien und Öffentlichkeit bestehen sollte, um Cyberkrieg und IT-Sicherheit zum politischen Thema zu machen. Die Unterstützung beginnt damit, konkrete Schutzwerkzeuge zu nutzen und – etwa mit PGP-Partys – bekannter zu machen. Der Beitrag von *Karin Schuler* in diesem Heft gibt dazu einen guten Überblick.

Fazit dieser Analyse und der Diskussion der Arbeitsgruppe war, dass weder die rechtlichen Grundlagen und Erfordernisse eines Cyberkrieges durch Geheimdienste noch die technischen Möglichkeiten für Reaktionen auch nur ansatzweise analysiert sind, jede politische Gestaltungsidee fehlt. Diese Defizite im Problembewusstsein haben leider zur Vernachlässigung von Lösungsansätzen und Visionen geführt. Visionen aber sind überfällig: Schließlich hat die brutale Realität des Krieges Abkommen wie die Genfer Konvention oder die Biowaffen- und Chemiewaffen-Konventionen nicht verhindert, sondern erst dazu geführt. Wenn es von staatlicher Seite kein Einsehen und keine Lösungen gibt, werden IT-Sicherheitsverantwortliche aus der Wirtschaft ebenso wie Bürgerinnen und Bürger genötigt sein, ihre Interessen gegenüber Politik und *Cyber-Kriegern* zu organisieren und umzusetzen. Aufgabe von kritischen Experten wie dem FIfF ist es, hier mitzuwirken.

Anmerkung

1 *Michael N. Schmitt (ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge, 2013*

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker, wissenschaftlicher Referent und Lehrbeauftragter an der FH Brandenburg.
Ute Bernhardt ist Informatikerin, wissenschaftliche Referentin und Lehrbeauftragte. Beide sind ehemalige Vorstandsmitglieder im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. und arbeiten zu Datenschutz, IT-Sicherheit sowie Informatik und Militär.