in Hand. Zugleich sind die US-Armee und die Geheimdienste damit auf Analysewerkzeuge angewiesen, die die richtigen Punkte in der schier unendlichen Masse an Informationen finden und miteinander verbinden können.

Fest steht damit auch, dass der cyber-militärische Komplex weiter anwächst – und nach und nach den militärisch-industriellen Komplex ablösen wird, der seine Wurzeln in den 1950er-Jahren hat. Allein in diesem Jahr stehen dem US-Verteidigungsministerium 5,5 Mrd. US$ für Investitionen im Bereich der *Cybersicherheit* zur Verfügung. Ein Großteil davon wird ins sonnige Silicon Valley fließen – und damit in die smarte, neue Überwachungswelt.

Der Beitrag ist in *Wissenschaft & Frieden* 2015-2: *Technikkonflikte, Seite 27–30* erschienen.
http://wissenschaft-und-frieden.de/seite.php?artikelID=2042

Anmerkungen

1 *Steve Blank: The Secret History of Silicon Valley Part VI: Every World War II Movie was Wrong. steveblank.com, 27.4.2009.*
2 *Dazu auch: Nafeez Ahmed: How the CIA made Google. medium.com, 22.1.2015.*
3 *Douglas Edwards (2012): I'm feeling lucky: Confessions of Google Employee Number 59. Boston: Mariner Books.*
4 *Der US-Regierung bietet Google zudem für 6,7 Mio. US$ seine Cloud-basierten E-Maildienste an. Vor diesem Hintergrund ist wenig verwunderlich, dass Länder wie Russland oder China Googles Dienste aussperren; vgl. dazu: Evgeny Morozov: Who's the true enemy of internet freedom – China, Russia, or the US? The Guardian, 3.1.2015.*
5 *Seit 2010 bietet Google der NGA zudem für 27 Mio. US$ „geospatial visualization services" an. Den Auftrag erhielt Google direkt und ohne Ausschreibung, was die NGA damit begründete, dass sie bereits erhebliche Investitionen in die Google-Earth-Technologie getätigt habe, die man nicht verlieren wolle.*
6 *Google Earth Builder supports NGA geospatial efforts. Official Google for Work Blog, 20.4.2011.*
7 *Das Geld, mit dem Keyhole vor der Pleite gerettet wurde, kam allerdings von der NGA. Die NGA verfügt über ein etwa halb so großes Budget wie die NSA; damals gab sie an, das Geld anstelle der »Intelligence Community« zur Verfügung zu stellen.*
8 *Ellen Nakashima: Google to enlist NSA to help it ward off cyberattacks. The Washington Post, 4.2.2010.*
9 *Google arbeitet auch eng mit Rüstungsunternehmen wie Lockheed Martin und Northrop Grumman zusammen. Lockheed erhielt von Google »geospatial technologies«.. Northrop zahlte rund eine Million US$ für eine maßgeschneiderte Google-Earth-Anwendung.*
10 *Yasha Levine; The revolving door between Google and the Department of Defense; pando.com, 23.4.2014. Jeremy Scahill: Blackwater for Sale. The Nation, 8.6.2010.*
11 *Derzeit verfügt gerade einmal gut ein Drittel der Weltbevölkerung über einen Zugang zum Internet: Vgl. den Bericht der Internationalen Fernmeldeunion ITU (2014): Measuring the Information Society Report 2014. Genf.*
12 *Daneben unterhält Palantir ein weiteres Dutzend Büros in der ganzen Welt, unter anderem in Tokio, Sydney, Singapur und Tel Aviv.*
13 *Siobhan Gorman: How Team of Geeks Cracked Spy Trade. The Wall Street Journal, 4.9.2009.*
14 *Palantirs Software ist damit das kommerzielle Gegenstück zum NSA-Tool XKeyscore. Mit ihm kombiniert und durchsucht der Geheimdienst Telekommunikationsdaten aus verschiedenen Quellen. Aus diesem Grund sehen Bürgerrechtsorganisationen wie die American Civil Liberties Union in Palantir auch einen „wahren totalitaristischen Albtraum", da die Software es ermögliche, das Leben unschuldiger Amerikaner in nie gekanntem Ausmaß zu überwachen. Andy Greenberg and Ryan Mac: How A »Deviant« Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut. Forbes, 2.9.2013.*
15 *Rowan Scarborough, Military leaders urgently push for new counter-terrorism software. The Washington Times, 27.8.2012.*
16 *Ryan Mac: National Security Darling – Why Condoleezza Rice, David Petraeus and George Tenet Back Palantir. forbes.com, 19.8.2013.*

Gertrud Maria Vaske

Cyberwar – die digitale Front: Ein Angriff auf Freiheit und Demokratie?

Interview mit Felix *FX* Lindner, Hacker

Felix *FX* Lindner *legte die Energieversorgung der Stadt Ettlingen lahm und hackte Blackberry sowie die Netzwerkstruktur von Cisco. Als ausgewiesener Experte in der Computer-Security-Szene präsentiert* „FX" *seine Forschungsergebnisse bereits seit über zehn Jahren weltweit auf Konferenzen und macht sie frei im Netz zugänglich. Er ist Gründer, technischer und Forschungsleiter von* Recurity Labs GmbH, *einem Beratungs- und Forschungsunternehmen für IT-Sicherheit im High-End-Bereich, das sich auf Code-Analyse und das Design von sicheren Systemen und Protokollen spezialisiert hat. Das Interview führte* Gertrud Maria Vaske.

Gertrud Maria Vaske (GMV): *Was ist Ihrer Meinung nach die größte Bedrohung im Cyberwar? Was war Ihrer Meinung nach die größte Bedrohung für Datensicherheit und Datenschutz im Jahr 2014?*

Felix *FX* Lindner (FX): Die größten Bedrohungen erwachsen meiner Meinung nach durch den Mangel an Verständnis bei vielen der verantwortlichen Personen. Dadurch bestimmten in 2013 und 2014 einige wenige Personen das mediale Narrativ und die politische Agenda. Eine sachliche Diskussion über Datensicherheitsstrategien ist leider so selten wie sie dringend angeraten ist.

GMV: *Welche Cyberwar-Gefahren gibt es vor allem militärisch, aber auch für die Privatbevölkerung und für Unternehmen?*

FX: Das Hauptproblem in allen drei Bereichen ist die blinde Digitalisierungswut. Wir schaffen es nicht, unsere existierenden Computersysteme und Netzwerke abzusichern, bauen aber überall noch mehr und tiefer vernetzte Computer ein, sei das nun in Waffensysteme oder Versorgungsinfrastruktur für Strom, Wasser oder Gas. An vielen Stellen ist der Nutzen bestenfalls ein Mythos, die zusätzlichen Gefahren sind aber sehr reell.

GMV: *Mit Cyberattacken können Waffensysteme wie z. B. Flugabwehrraketen lahm gelegt werden. Warum wird das so selten gemacht?*

FX: Einerseits ist das notwendige Wissen und Personal mit den entsprechenden Fähigkeiten dünn gesät. Solange man konventionelle Mittel zur Verfügung hat, um den gleichen Effekt zu erzielen, lohnt sich der Einsatz dieser knappen Ressource nicht. Zum anderen haben die verantwortlichen Personen in Militär und Politik aufgrund ihres mangelnden Fachwissens auch eine berechtigte Angst vor Sekundäreffekten, welche sie nicht einschätzen können.

GMV: *Könnte man mit Cyberattacken die aktuellen Konflikte (Syrien/Ukraine) eindämmen?*

FX: Cyberattacken sind für diesen Zweck ungeeignet. Offensivmittel sind ja generell eher das falsche Mittel der Wahl, um Konflikte zu entschärfen.

GMV: *Sollte ich als Verteidigungsministerin lieber in Cyberwaffen oder Cybersicherheit investieren oder lieber in herkömmliche Waffen?*

FX: Das sollte ein Ergebnis einer sicherheitspolitischen Gesamtstrategie sein, welche eine Verteidigungsministerin hoffentlich hat. Der Aufbau von Offensivfähigkeiten *on par* mit denen anderer Länder ist sicherlich ein Muss, denn die fünfte Domäne wird nicht einfach wieder verschwinden, und genauso wie man keine Luftwaffe vom einen Tag zum anderen bei *Amazon* bestellen kann, so müssen auch Cyberoffensivkräfte viele Jahre trainieren, bevor sie einsatzbereit sind. Die sogenannte Cybersicherheit ist eher eine gesamtpolitische Aufgabe.

GMV: *Was brauche ich, um die Infrastruktur eines Landes lahm zu legen?*

FX: Bezogen auf einen Cyberangriff reichen hier ein paar fähige Angreifer mit schiefem moralischem Kompass und das entsprechende Geld, um diese zu bezahlen. Hat man es aber nicht eilig damit, bietet sich auch umfangreiche Privatisierung als ein sehr effektives Mittel an.

GMV: *Aufsehen haben die Cyberwaffen* Stuxnet *und* Flame *erregt. Damit wurde das iranische Atomwaffenprogramm ausgespäht und angegriffen. Was war daran besonders gefährlich?*

FX: Besonders gefährlich daran sind die Kollateralschäden – und zwar nicht die direkt ersichtlichen. Beispielsweise wurde für *Flame* eine kryptographische Signatur erzeugt, damit es so aussah, als ob die Datei von *Microsoft* selbst kam. Dadurch wurden viele Sicherheitsprüfungen umgangen, welche essenziell für eine ganze Reihe von Schutzmaßnahmen in der Computersicherheit sind. Diese Methode funktioniert auch heute noch, die Schutzmaßnahmen können aber nicht einfach mal ausgetauscht werden. Dadurch wurde die ganze Welt verwundbarer als sie es vorher war.

GMV: *Entmystifizierung des Cyberwar – oft heißt es, den gebe es nicht und der sei nicht neu. Sie haben auf unserer Berliner Podiumsdiskussion zu der Behauptung, Schadsoftware trüge keine Uniform, gesagt, die militärischen Angriffe im Netz trügen mehr Uniform als russische Soldaten auf der Krim – was meinen Sie damit genau?*

FX: Fast alle Staaten haben wenig Hoffnung auf mittelfristig verfügbare Defensivmaßnahmen und konzentrieren sich daher auf Offensivmittel. Dementsprechend soll allen anderen gezeigt werden, was man kann, also eine Art *Show of Force*. Die Hoffnung ist, einen gewissen Grad von Abschreckung zu erreichen. Dazu muss aber offensichtlich sein, von wem der Angriff entwickelt und durchgeführt wurde. Es wird also wenig verschleiert.

GMV: *Wieviel Cyberpower hat China oder Russland im Vergleich zu den USA?*

FX: China und Russland sind offensiv vergleichbar stark wie die USA, wenn auch in jeweils etwas anderer Ausprägung.

GMV: *Wer sind derzeit die Cybersupermächte?*

FX: *Google*, China, Russland und die USA.

GMV: *Also Länder, die selbst Computer bauen, haben gute Chancen, Cyberpower zu sein oder zu werden. Wie stehen da derzeit die Chancen für Deutschland? Werden wir nach Zuse überhaupt noch computertechnisch wahrgenommen in der Welt?*

FX: Nein, Deutschland spielt hier keine besondere Rolle mehr. Das ist besonders schade, da die Fähigkeiten durchaus vorhanden sind, aber leider nicht genutzt werden.

GMV: *Wie gehen Cyberangreifer vor? Was tun sie, wenn sie ein Land, Konzerne, Firmen, den Staat oder den Geheimdienst angreifen wollen?*

FX: Der Vorgang ist grob vergleichbar mit einem Einbruch: Hintergrundinformationen beschaffen, auskundschaften, an Türen und Fenstern rütteln, Werkzeuge auswählen und dann den Einbruch durchführen. Im Unterschied zu einem Einbruch flüchtet man nicht danach, sondern verbarrikadiert sich möglichst unauffällig im Objekt.

GMV: *Welche Abwehrmechanismen gibt es, um sich gegen Eindringlinge zu wappnen? Müssen wir nicht eigene Computer bauen?*

FX: Ja, wir müssten wirklich eigene Computer bauen. Wenn wir für diese im Unterschied zu allen anderen auch eine Produkthaftung übernehmen würden, wären sie zwar deutlich teurer, aber auch der Exportschlager schlechthin.

GMV: *Gibt es ein Patentrezept gegen Cyberangreifer, z. B. wieder auf Schreibmaschine umzustellen?*

FX: Wenn Sie ein Geheimnis bewahren wollen, sollten Sie es heutzutage nicht in einen Computer stecken.

GMV: *Blicken wir auf das kommende Jahr. Nationalstaaten, die sich mehr und mehr gegenseitig mit Schadsoftware angreifen. Der jeweilige Privatsektor ist betroffen und auch Aktivisten werden das Internet weiterhin für eigene Zwecke nutzen – was wäre der „Supergau" für Deutschland? Welches Szenario könnte schnell wahr werden?*

FX: Deren gibt es leider viele. Ich vertrete aber die Auffassung, dass man keine Anleitungen öffentlich zur Verfügung stellen sollte.

GMV: *Wie kann man ein solches Szenario verhindern?*

FX: Eine gesamtpolitische Auseinandersetzung mit dem Thema wäre ein erster Schritt.

GMV: *Kann man mit einem anständigen Computer einen Flughafen lahmlegen? Nennen Sie uns bitte eine grobe Schätzung. Wie viele Menschen können das Ihrer Meinung nach?*

FX: Einige tausend Personen weltweit sind es bestimmt.

GMV: *Manche Stimmen werden lauter: Panikmache und Forderung nach Aufklärung – worin sehen Sie die Aufgaben von Produzenten von Soft- und Hardwareprodukten, um die Computersicherheit zu verbessern?*

FX: Es wäre schön, wenn die Produzenten endlich ehrlich zur Politik wären. Immer neue Versprechen vom nächsten Wundermittel bringen uns nicht weiter. Das Eingeständnis, dass die nicht vorhandene Haftung ihrerseits das Kernproblem darstellt, würde eine Menge ändern. Die Politik wird nicht sofort eine solche Haftung fordern, denn niemand will SAP & Co. ruinieren. Doch leider ist die momentane Scharlatanerie zu einträglich, als dass sie freiwillig aufgegeben würde.

GMV: *Laut Thomas Ried ist Cyberwar nur eine clevere Strategie von Sicherheitsfirmen, denn eigentlich gibt es ihn seiner Meinung nach nicht. Was halten Sie von der Ried-These?*

FX: Der Begriff *Cyberwar* eignet sich ausgezeichnet, um den Verkauf des nächsten Wundermittels anzukurbeln. Er erklärt aber weder die Hunderte von Soldaten und die Horden von Experten in der Verteidigungsindustrie verschiedener Länder, die sich mit dem Thema Offensivkapazitäten befassen, noch die großen Summen in den entsprechenden Etats. Herr Ried beschreibt ein Symptom, nicht die Krankheit.

GMV: *Wie schätzen Sie die Sicherheitslage deutscher Firmen generell ein?*

FX: Deutsche Firmen sind meiner Meinung nach hochgradig exponiert. Wir sind ein Exportland, spezialisiert auf Prozess- und Produktionswissen. Anders als Rohstoffe ist unser Exportgut also perfekt geeignet, um aus unseren Computern entwendet (d. h. kopiert) zu werden, ohne dass wir es merken.

GMV: *Experten gehen davon aus, dass gezielte Hackerangriffe jährlich Schäden in Millionenhöhe verursachen – glauben Sie, dass die Mehrheit der CIOs und IT-Leiter derzeit in der Lage sind richtige und sinnvolle Schutzmaßnahmen zu ergreifen?*

FX: Nein, was unter anderem daran liegt, dass der CEO es zur Aufgabe des IT-Leiters macht, als hätte der CEO damit nichts zu tun.

GMV: *Wird Sicherheit künftig der Bequemlichkeit geopfert? Internet in Bundeswehrkasernen – wie sicher ist eine E-Mail-Adresse innerhalb der Bundeswehr vor Hackern?*

FX: Sicherheit wird immer der Bequemlichkeit oder Eitelkeit geopfert. Unternehmen haben jahrelang großen Aufwand betrieben, um mit *BlackBerry* eine halbwegs verlässliche Infrastruktur zu schaffen, und dann wollten die CEOs lieber *iPhones*. Die Sicherheit einer E-Mail innerhalb der Bundeswehr kann man einfach mal testen lassen. Leider wird auch das fast nie gemacht, denn die befürchtete Antwort will keiner hören.

GMV: *Wie sicher ist mein Smartphone (Samsung) vor Ihnen?*

FX: Vor mir ist es sicher. Ich habe kein Interesse daran.

GMV: *Manche Experten behaupten, dass es bislang keinen einzigen Cyberangriff gegeben hat. Trotzdem wird immer wieder vom Cyberwar gesprochen. Ist dies eine Strategie von Sicherheitsfirmen, Marketing- und Medienexperten und ist Cyberwar gar unreal?*

FX: Ob es Cyberangriffe gegeben hat, ist eine Definitionsfrage und daher strittig. Nationalstaatliche Aktivitäten nehmen allerdings definitiv kontinuierlich zu, das ist leider kein Marketing, so sehr ich mir das auch wünschen würde.

GMV: *Was macht einen guten professionellen Hacker aus?*

FX: Integrität, Passion, Fachwissen und Fähigkeiten sowie die Kirche im Dorf lassen.

GMV: *Müssen Hacker um ihr Leben fürchten bzw. wie zimperlich sind Geheimdienste?*

FX: Gewaltsame Todesfälle mit möglichem geheimdienstlichem Hintergrund sind eher selten bekannt geworden. Hacker, die für kriminelle Vereinigungen gearbeitet haben, werden schon häufiger mal tot aufgefunden, wenn der Job erledigt ist.

GMV: *Unterhalb der Schwelle eines bewaffneten Konflikts – was gibt es für einen Regelungsbedarf?*

FX: Wie gesagt sehe ich den größten Bedarf in der Einführung von Produkthaftungen für Hard- und Software, zumindest wenn die Produkte an den Staat oder das Militär geliefert werden. Solange es einträglicher ist, völlig kaputtes Zeug zu verkaufen, damit man dann auch noch die nächste Version verkaufen kann, gibt es kein Geld mit sicheren Computern zu verdienen, also baut sie auch keiner.

GMV: *Eine Frage nach dem Ausmaß und der Bedrohung durch Überwachung. Was würden Sie einem Regierungschef sagen, der* Google Mail *nutzt, mit dem* Google-*Browser* Chrome *surft und ein Smartphone mit dem* Google-*Betriebssystem* Android *benutzt?*

FX: Ich würde fragen, warum er oder sie das Geld der Bürger an Ministerien für Verteidigung, Spionage und Spionageabwehr verschwendet, da dieses Verhalten deren Arbeit *ad absurdum* führt. Außerdem würde mich interessieren, inwieweit der Amtseid mit einer fahrlässigen vollständigen Auslieferung des Staates an eine transnationale Supermacht vereinbar ist.

GMV: *NATO-Experten haben mit dem* Tallinn Manual *2013 ein Handbuch bereitgestellt, das sich mit der Anwendbarkeit des Völkerrechts im Cyberspace beschäftigt. Spielt das Handbuch bei Hackern eine Rolle?*

FX: Nein, das sind *Policy*-Fragen.

GMV: Google/Apple/Microsoft – *inwieweit sind diese Firmen eine Gefahr für die persönliche und nationale Sicherheit?*

FX: *Googles* Kontrolle über das gesamte Internet sollte bei Fragen der nationalen Sicherheit eine prominente Stellung einnehmen.

GMV: *Welche internationalen Cyberschutzgesetze brauchen wir?*

FX: Wir sollten internationale Regeln aufbauen, welche die Kontrolle über das Internet in der Hand der demokratischen Länder der Welt belassen, obwohl diese die Minderheit aller Länder darstellen.

GMV: *Und welche Gesetze, etwa zur Produkthaftung, brauchen wir für die Sicherheit von Computern oder Software?*

FX: Volle Produktlieferung (keine Lizenz) und entsprechende Produkthaftung für vom Bund oder der Bundeswehr beschaffte Software ist der erste und wichtigste Schritt. Nach chaotischen Anfängen werden Sie einen dramatischen Qualitätsanstieg bemerken, Sicherheit inklusive.

GMV: *Im Cyberangriffsfall, rein hypothetisch gefragt: Würden Sie im Tarnanzug für Deutschland hacken?*

FX: Ich helfe verschiedenen Ländern, ihre Infrastruktur besser zu verteidigen. Einen Tarnanzug habe ich dafür bis jetzt noch nie gebraucht.

Der Beitrag wurde übernommen aus *Ethik und Militär*, Ausgabe 2014/2 *Cyberwar – die digitale Front: Ein Angriff auf Freiheit und Demokratie?*, E-Journal-Special *(http://www.ethikundmilitaer.de/index.php?id=26).*

Gertrud Maria Vaske

Gertrud Maria Vaske ist Chefredakteurin des E-Journals *Ethik und Militär*.
vaske@zebis.eu

Reiner Braun und Lucas Wirl

Aufrüstung, Militarisierung und Rüstungsforschung an Hochschulen

Die Aussage Ban Ki Moons vor der NPT-Konferenz 2010, die Welt sei überrüstet und der Frieden unterfinanziert, trifft heute – 5 Jahre später – mehr zu denn je. Durch die globale Finanzkrise liegen die globalen, jährlichen Rüstungsausgaben zwar seit einigen Jahren stabil bei ca. 1,7 Billionen US-Dollar, jedoch verfällt die deutsche, europäische und internationale Politik in Praktiken und Gebaren, die nach zwei Weltkriegen und dem Wegfall des „Gleichgewichts des Schreckens" und des ideologisch bedingten Ost-West-Konfliktes überwindbar zu sein schienen: Deutschland stellt sich mit einer „Armee im Einsatz" zur Sicherung wirtschaftlicher Interessen als internationaler militärischer Faktor auf, der Krieg ist zurück in Europa – in der Ukraine und auch in Griechenland – und der global geführte „Krieg gegen den Terror" stellt in einer Reihe von Brüchen des Völkerrechts den wohl universellsten dar. Von der Illusion einer Friedensdividende musste schnell Abstand genommen werden.

In unserer multipolaren Welt ist die Schwelle militärischer Gewaltanwendung und Interessensdurchsetzung gesunken. Nach dem Kalten Krieg und den kurzen Jahren der Kooperation befinden wir uns in einer Phase der Konfrontation mit der Tendenz zu einer Neuaufteilung der Welt, die (bisher) durch hohe Komplexität und Unübersichtlichkeit geprägt ist. Ein Ausdruck dessen ist eine neue Rüstungsspirale und eine Militarisierung der Außen- und Innenpolitik.

Eine neue Rüstungsspirale und Revolutionen des Militärwesens

Aus Obamas berühmter Rede in Prag ist nur noch „but not in my lifetime" in bitterer Erinnerung geblieben, und die Welt befindet sich heute in einer neuen Rüstungsspirale. An oberster Stelle, angeführt von den USA und der NATO, ersetzen alle Atomwaffenstaaten ihre nuklearen Arsenale durch hochmoderne High-