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

Ute Bernhardt und Ingo Ruhmann

Das Blaumilch-System

Der unerklärte *Information Warfare*

1940 knackten die Briten erstmals mit programmierbaren Rechnern die deutsche ENIGMA-Verschlüsselung. Dieses Wissen wurde bis 1974 als Staatsgeheimnis gehütet. In den dazwischenliegenden 30 Jahren wurde die auf der ENIGMA beruhende kompromittierte Verschlüsselungstechnik weiter von staatlichen Stellen genutzt – und von den Briten geknackt. Dank Edward Snowden haben die Angreifer heute diesen Zeitvorsprung verloren. Wenig mehr als zehn Jahre nach der Entwicklung von digitalen Überwachungs- und Angriffswerkzeugen wie Turmoil, Turbulence *und deren Schwestersystemen wie* XKeyscore *wissen wir heute, in welchem Umfang Datenkommunikation weltweit überwacht und Computer mit solchen Werkzeugen angegriffen und manipuliert werden. Was macht den Unterschied aus?*

Otto Leiberich, lange Jahre Leiter der westdeutschen Zentralstelle für das Chiffrierwesen und nach deren Umwandlung in das Bundesamt für Sicherheit in der Informationstechnik (BSI) auch dessen erster Präsident, konnte sich noch in den 90er-Jahren im Verlauf von Interviews, Gesprächen und in Beiträgen mächtig darüber echauffieren, dass erst 1974 bekannt wurde, dass das ENIGMA-Verschlüsselungsverfahren kompromittiert war[1]. Heute sorgt es hingegen kaum noch für Aufregung, dass aktuelle und ehemalige Kabinettsmitglieder im Dutzend und Regierungsmitarbeiter in Kohortenstärke abgehört wurden, dass Verschlüsselungsverfahren und grundlegende IT-Sicherheitsmechanismen ausgehebelt sind. Und dass das alles nicht einmal bemerkt wurde.

Liegt es daran, dass zum Glück kein Krieg mehr herrscht und Politiker sowieso all ihre Kommentare an die Medien geben? Und wir alle dann weiter nur das Glück haben, diese ungefilterte Mitteilungswut der Politik nicht erdulden zu müssen, weil wohlmeinende Journalisten uns nicht damit behelligen? Oder liegt es doch eher daran, dass Politiker auch nur Menschen sind und mit vielerlei missliebigen und politisch inkorrekten Äußerungen aus vielfältig belauschter Kommunikation genauso kompromittierbar sind wie ihre IT-Systeme? Was sollten denn sonst die Anlässe und Motive für die lange Zeit unerkannten Angriffe auf die Server des Deutschen Bundestages sein, wenn nicht die aus der Überwachung gewonnenen Kenntnisse über Absprachen oder persönliche – digital übermittelte – Äußerungen von Politikern, die nicht mit deren öffentlicher Kommunikation übereinstimmen?

Das Schöne Neue daran ist: Wir werden es erfahren! Und zwar nicht erst in 30 Jahren, sondern bei passender Gelegenheit. Denn zur Kernkompetenz der Geheimdienste gehört nicht nur das Ausspähen, sondern auch das Nutzen der erlangten kompromittierenden Informationen.

Der Rücktritt von Roderich Kiesewetter, CDU-Obmann im NSA-Untersuchungsausschuss, wegen BND-Informanten in seinem Umfeld – oder doch wegen russischer Agenten? – lupft die Decke ein ganz kleines Stückchen von diesem schmuddeligen Tun[2]. Zum Vorschein kommt die munter betriebene Manipulation des politischen Betriebs durch die Dienste, zum Vorschein kommen

düpierte Abgeordnete, die sich von Geheimdiensten in der Ausübung ihres Mandates auch zu Recht manipuliert sehen.

Abgehörte und durch das erlangte Wissen kompromittierbare Beamte könnten keine Sicherheitsüberprüfung überstehen. Diverse Kabinettsmitglieder, nach dem gleichen Muster als Geheimnisträger bewertet, dürften nicht einmal ihre eigenen Kabinettssachen lesen, weil sie nicht durch die Sicherheitsüberprüfung kämen – zum Glück aber gelten die Regeln für den Beamtenapparat nicht für sie.

Dumm nur, dass sich nicht nur der politische Betrieb Berlins vor der Fremdsteuerung ängstigt. Auch wir Bürgerinnen und Bürger werden manipuliert – durch jene Medienberichte, die dunkle Quellen zu genehmer Zeit lancieren, um politische Karrieren zu stutzen oder zu verändern: Medial von gezielt gestreuten Meldungen manipulierte WählerInnen sind das Gegenstück zu kompromittierten Politiker.innen.

So geht Information Warfare.

Und damit gilt es, noch einen weiteren Irrtum auszuräumen. Denn natürlich herrscht Krieg – Informationskrieg. Darin macht es keinen Unterschied, ob wahre Meldungen belauscht und zur rechten Zeit publiziert werden, oder ob Falschmeldungen kunstvoll fabriziert und an die Medien lanciert werden.

Das heutige politische Italien zeigt unsere Zukunft: Nach dem Klima des politischen Misstrauens aus Unkenntnis folgten eine Welle von publizierten Abhörprotokollen aus unterschiedlichsten Quellen und entsprechende Skandale. Das Ergebnis ist heute der Wunsch nach Ehrlichkeit, Purismus und Klarheit – den letztlich aber nur Populisten und sektiererische Ideologen in Reinkultur liefern können, solange die geheimen Manipulateure der öffentlichen Meinung ungestört weiter arbeiten können.

Offenheit und Klarheit in der Politik ist gut. Aber sie stört den politischen Aushandlungsprozess. Denn Politik beruht auf Aushandlung und Kompromissen. Bis Kompromisse erzielt sind, sind notwendigerweise die Verhandlungen zwischen gegensätzlichen Positionen erforderlich. Die inhaltliche Differenz solcher Verhandlungen ist das Spielfeld für Manipulation und Kompromittierung. Ideologen und Populisten dagegen verhandeln nicht. Sie sind nicht kompromittierbar, wenn sie nicht verhandlungs- und kompromisswillig sind.

Die Kompromittierung von Politiker.innen durch die Kompromittierung ihrer IT-Systeme untergräbt die Möglichkeit der Verhandlung und des Kompromisses. Die Kompromittierung liegt im Interesse einer der Parteien im Verhandlungsprozess. Sie hebelt zum Nachteil anderer die Verhandlungen aus.

So geht Information Warfare.

Das zu leugnen und sich stattdessen zum Spielball derer zu machen, die Kompromisse und politisches Handeln in ihrem Sinne manipulieren wollen, ist ein schädliches Versagen von Politik und Medien zugleich. Denn Bürgerinnen und Bürger verstehen durchaus die aufgabenbedingte Doppelbödigkeit von Politik und schätzen auch kluge politische Schachzüge. Sie schätzen aber nicht Feigheit und Unehrlichkeit gegenüber Fakten und Zwängen. Manipulation im *Information Warfare* ist ein solches Faktum und schafft Zwänge.

Doch die heutigen Spielbälle der Dienste – genau: unsere Politiker.innen, deren PARLAKOM-Netzwerk im Bundestag so verwurmt ist, dass es aufgegeben werden muss – wollen sich zu Spielern wandeln. Regierungsmitglieder sind digital nackt, das Parlament digital handlungsunfähig und seiner Infrastruktur beraubt – man könnte fast sagen: Opfer eines digitalen Enthauptungsschlages – und doch wollen beide nicht nur etwas mehr Schutz für ihre IT-Systeme, sondern vor allem mehr Personal und Technik für den Angriff auf die IT-Systeme anderer. Gut möglich, dass die Dienste der potenziellen Zielländer dieser Angriffe schon die Cyberwar-Pläne gelesen haben, bevor sie von Regierung und Parlament beraten und verabschiedet sind. Egal.

Mit dem IT-Sicherheitsgesetz verbessert sich allein die Lage für die IT des Bundes durch BKA-Sonderermittler, durch mehr Personal beim BSI und mehr Personal im Bundesamt für Verfassungsschutz – letzteres heute schon auf besondere Weise bekannt für seine Variante einer „Cyberspionage-Abwehr“ gegen NSA, GCHQ und andere. Vom BND weiß man nicht, ob er sich vielleicht sogar durch falsch selektierte Selektoren auch noch als Cyberspion-Gehülfe im eigenen Haus herausstellt. Davon ungerührt rüsten BND und Bundeswehr derweil auf: Der BND beantragt zehnmal mehr Mittel für Personal, Wissen und Mittel für Cyberangriffe als die Bundesregierung pro Jahr für die IT-Sicherheitsforschung zur Verfügung stellt. Das Verteidigungsministerium arbeitet an einer Strategie für Cyberangriffe der Bundeswehr und hat eine „Strategische Leitlinie“ erlassen[3].

Das ist Information Warfare.

Ist das auch klug? Und selbst wenn man an die Richtigkeit von Krieg glauben würde, muss sich jeder Stratege fragen: Lässt sich damit etwas gewinnen? Strategie – nur zur Erinnerung – ist der zielgerichtete Einsatz meist militärischer Gewalt oder die Gewaltandrohung zur Erreichung politischer Ziele. Wenn man also glaubt, militärisch aktiv werden zu müssen: Was ist die Information-Warfare-Strategie der Bundeswehr?

Denn um Gewinnen geht es. Für die Verteidigung hat die Bundeswehr seit Jahren das CERTBw. Das ist die zur Abwehr konkreter Angriffe gerufene Einheit, die öffentlich seit mindestens 2007 erklärt, dass auch befreundete Nachrichtendienste die Netze der Bundeswehr angreifen. Und weil es von der Arbeit von Zivilisten und seiner Mitgliedschaft im CERT-Verbund abhängig ist, ist das CERTBw beim IT-Amt der Bundeswehr angesiedelt und strikt getrennt von den Cyber-Angreifern im Kommando Strategische Aufklärung (KSA).

„Offensive Cyber-Fähigkeiten der Bundeswehr haben grundsätzlich das Potenzial, das Wirkspektrum der Bundeswehr in multinationalen Einsätzen signifikant zu erweitern“, so die neuen Leitlinien des BMVg. Was also will die Bundeswehr im *Information Warfare* gewinnen? Und gegen wen? Um welchen Krieg geht es dabei genau? Wer hat den erklärt? Unter welcher Flagge führt die Bundeswehr diesen? Das Verteidigungsressort erklärt *False-Flag*-Aktionen als „Kriegslist“ für zulässig[4]. Und der Angriff auf zivile Netzwerke? Auch das ist nach Ansicht des zuständigen Parlamentarischen Staatssekretärs zulässig[5].

Oder wollen auch die Bundeswehr oder die Bundesregierung mitmischen im Spiel der Kompromittierung, der Ausspähung und Manipulation, der Falschmeldung und Sabotage? Und geht es gar um die Manipulation physischer Systeme – die Fernsteuerung der Autos und Flugzeuge von *Value Targets* – oder um die Destruktion von Maschinen und Anlagen?

Information Warfare ist eine Strategie für ein garantiertes Desaster moderner Gesellschaften. Verantwortungsvolle Zeitgenossen – auch solche, die sich in Uniform mit diesem Thema praktisch beschäftigt haben – konzentrieren sich auf Begrenzung und Abwehr. Wer daran glaubt, als konventionelle Streitkraft mit *Information Warfare* irgendetwas gewinnen zu können, sollte mindestens erkennen lassen, welche Antworten er oder sie für die Fragen und Probleme bedacht hat, die sich aus einer solchen Strategie ergeben.

Derzeit beschleicht den oberflächlichen Betrachter aber das ungute Gefühl, dass hier ebenso wenig überlegt wird wie zu Beginn des Ersten Weltkriegs auf allen Seiten – oder zu verschiedenen Zeiten im Zweiten Weltkrieg, als polnische Ulanen zu Pferd gegen angreifende deutsche Panzer anritten, Rotarmisten zu Beginn des Krieges oder der Volkssturm an dessen Ende jeweils ohne Waffen gegnerische Panzer aufhalten sollten. Immerhin wird der Wahnsinn für jeden greifbarer, wenn man Panzer sehen, hören und intensiv spüren kann. Bei Bits und Bytes ist die Vermittlung derselben Fakten wohl etwas schwieriger.

Die Bundesregierung will ihre Rechenzentren konsolidieren und kommt den Angreifern mit der Zentralisierung der Ziele sehr entgegen. Ist das hoffnungslos naive Feindesliebe oder soll mit dem republikweit größten Honeypot für Cyberkrieger eine besonders gekonnte Strategie verbunden werden?

BND und Verfassungsschutz haben die von der NSA entwickelte integrierte Cyberwar-Softwaresuite *XKeyscore* eingesetzt[6]. Angeblich erkannten beide aber nicht, welche Cyberwaffe sie da nutzen. Ist das eine dreiste Lüge oder die Wahrheit? Und welche dieser zwei Möglichkeiten ist die bessere Variante?

BND und Verfassungsschutz haben trotz des Wissens um Cyberangriffe von „befreundeten Diensten" die Angreifer weder verfolgt noch eingegrenzt. Auch für die Zukunft ist nicht zu erkennen, dass die in Deutschland verantwortlichen Cyberkriegs-Akteure ihre angreifenden Gegner überhaupt erkennen.

Bei genauer Betrachtung erstaunen die *Information-Warfare*-Krieger in Deutschland auf allen Ebenen. Sie haben keine Strategie. Sie können keine Ziele ihres Tuns benennen. Sie erkennen keine Angriffe auf die politischen Spitzen des Staates und das gesamte Parlament. Sie erkennen weder ihre Gegner, noch deren Waffen. Sie leisten keinen Beitrag zur politischen und militärischen Sicherheit und schon gar nicht zur IT-Sicherheit – letzteres leistet seit langem eine nach zivilem Muster aufgebaute CERT-Einheit der Bundeswehr. Sie riskieren stattdessen mit ihrem Tun ihre eigene Infrastruktur und die der Zivilgesellschaft. Sie drohen, politische Krisen durch ihr Tun militärisch zu eskalieren.

Wenn man zurück kommt zu den Ausgangsfragen und wenn man dabei an die Richtigkeit von Krieg glauben würde, wird sich jeder Stratege angesichts dieser Lage nur an den Kopf fassen wollen. Statt Mittel zu investieren, um die erkannten Probleme zu lösen, wird für jene Geld bereitgestellt, die umfassend bewiesen haben, dass sie von sicherer IT im Zivilleben und der IT in der Welt der heutigen Geheimdienste zwar frei von Kenntnissen sind, aber leider nicht frei von Wünschen.

Zurück zur ENIGMA. Ihre Entschlüsselung war ein Staatsgeheimnis, das Jahrzehnte von höchster strategischer Bedeutung war. Die meisten Staatsgeheimnisse sollen aber nur die Schwächen und vor allem das untaugliche Tun von verantwortlich Handelnden im Staate verheimlichen. Legt man diese Auslegung der Facetten der Ausspähung und des *Information Warfare* zugrunde, so darf sich niemand mehr ernsthaft fragen, warum der NSA-Skandal und seine Details mit allen Mitteln geheim gehalten werden müssen.

Loriot hat wunderbare Satiren über Konstellationen geschrieben, in denen ein starrköpfiges Familienmitglied einfach irgendein verrücktes „Dings" haben oder machen musste. Ebenso treffend ist Ephraim Kishons „Blaumilchkanal" über einen aus der Heilanstalt entflohenen Verrückten, der die Straßen einer Stadt nacheinander mit dem Presslufthammer aufmeißelt, wobei das Versagen, ihm Einhalt zu gebieten, am Ende als genialer staatlicher und politischer Plan verkauft wird.

Der Blaumilchkanal ist heute noch lustig. *Information Warfare* ist genauso verrückt. Nur lustig ist daran nichts.

Ingo Ruhmann und Ute Bernhardt

Ingo Ruhmann ist Informatiker und arbeitet im Bereich Technikfolgenabschätzung, Forschungspolitik, IT-Sicherheit, Information Warfare, *Cyberwar*, Geschichte der Geheimdienste und Datenschutz. Er ist Lehrbeauftragter im Studiengang *Security Management* der Fachhochschule Brandenburg. Er ist Mitglied des FIfF und war Vorstandsmitglied von 1991 bis 1998.

Ute Bernhardt ist Informatikerin und beschäftigt sich seit Jahren mit Forschungspolitik, Datenschutz und IT-Sicherheit, dem Verhältnis von Wissenschaft und Frieden sowie der Beziehung von Informatik und Militär. Sie hat Lehraufträge an der Fachhochschule Bonn-Rhein-Sieg und der FernUni Hagen. Sie ist Mitglied des FIfF und war FIfF-Vorstandsmitglied von 1991 bis 1998.

Anmerkungen

1 *Vgl. etwa: Otto Leiberich: Vom diplomatischen Code zur Falltürfunktion. In Spektrum der Wissenschaft, 01.06.1999. Vgl. auch: http://www.spektrum.de/magazin/vom-diplomatischen-code-zur-falltuerfunktion/825487*

2 *Politiker im NSA-Ausschuss verlangen Aufklärung. Die Welt, 08.02.2015, http://www.welt.de/politik/deutschland/article137244296/Politiker-im-NSA-Ausschuss-verlangen-Aufklaerung.html und: Verwirrung komplett. Süddeutsche Zeitung, 21.07.2015, http://www.sueddeutsche.de/politik/nsa-ausschuss-verwirrung-komplett-1.2575592?reduced=true*

3 *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, dokumentiert unter: https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung*

4 *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan van Aken, Andrej Hunko, Christine Buchholz, weiterer Abgeordneter und der Fraktion DIE LINKE, „Elektronische Kampfführung der Bundeswehr", BT-Drs. 18/3963, Antwort auf Fragen 30–33*

5 *Plenarprotokoll der Fragestunde der 16. Sitzung des Deutschen Bundestages vom 19.02.2014, Antwort auf Frage 8, S. 1165 f.*

6 *Schnüffelsoftware XKeyscore: Deutsche Geheimdienste setzen US-Spähprogramm ein. SPIEGEL ONLINE, 20.07.2013, http://www.spiegel.de/politik/deutschland/bnd-und-bfv-setzen-nsa-spaehprogramm-xkeyscore-ein-a-912196.html*

Florian Mehnert

Das Kunstexperiment *11 TAGE*

Die gezielte Tötung als Konsequenz einer totalen Überwachung

Die Installation 11 TAGE

Nach den vorhergehenden Kunstprojekten, die sich vor allem mit der Veranschaulichung der Überwachung auseinandersetzen, ging es mir wieder darum, eine Arbeit zu schaffen, in der die Folgen der Überwachung deutlich werden, aber hier vor allem, dass der Rezipient selbst partizipieren kann. Es war mir wichtig, dem Rezipienten eine entscheidende Rolle zu geben, ihn in eine kritische Situation zu bringen, in der er selbst Überwacher und Entscheider ist.

Der Aufbau

Die Installation *11 TAGE* besteht aus einer weißen Polyethylen-Box mit den Maßen 150 x 60 x 60 cm³. In der Box ist ein Rattengehege eingerichtet, in dem sich eine lebende weiße Ratte befindet. Die Box steht auf einer Stahlkonstruktion, an der eine über das Internet steuerbare Waffe angebracht ist. Die Rückwand der Box ist auf 4 cm verstärkt, um den Projektilen der Druckluftwaffe zu widerstehen. Drei Servomotoren sind für die Bewegung und das Auslösen der Waffe zuständig. Diese Motoren werden über ein *Arduino*-Board geregelt, das per USB-Verbindung mit einem Computer verbunden ist. Auf dem Waffenlauf ist eine Webcam montiert. Die gesamte Installation ist 195 cm lang, 60 cm breit und 145 cm hoch.

Auf dem dazugehörigen Computer befinden sich Skripte, die das Kontrollieren der Waffe über die Internetseite ermöglichen und den Lifestream im Internet auf dem Server bereitstellen. Die