Militärisches Sperrgebiet Internet

vom mobilen Interviewkommando <ds@ccc.de>

Mit dem aufkommenden Mythos „Cyberwar“ muß sich die Redaktion Datenschleuder nun schon seit einiger Zeit herumschlagen. Nun ist es uns gelungen, den bedeutendsten Kybernetikkriegsberater der NATO zum Thema zu interviewen. Lesen Sie hier eine exklusiven Vorabdruck unseres Interviews mit dem Cyberwarspezialexperten Major a. D. Georg-U. U., Nato-Berater für strategische Fragen, Stabsabteilungsleiter Militärpolitik a. D., Fellow der Deutschen Atlantischen Gesellschaft.

Datenschleuder: *Herr U. U., Sie haben die Führung des Government Service Cyberwar Center ... wie sagt man eigentlich auf Deutsch? ... des Kybernetikkriegsregierungszentrums der deutschen Streitkräfte beraten, wie sie die deutschen Handelswege und Rohstoffinteressen auch in den digitalen Netzen vor kriegerischen, terroristischen und piratigen Angriffen verteidigen können.*

Zuerst die Frage: Was denken Sie, ist der wichtigste Grund für das Militär, auch im Internet Stärke und Präsenz zu zeigen?

U. U.: Der Charakter des aufziehenden Cyber Warfare verändert die strategische Ausrichtung unserer Heimatarmeen in dem Maße, wie die Vernetzung Einzug in die Waffengattungen nimmt. Das im vorigen Jahr mit meiner Hilfe verabschiedete neue strategische Konzept der NATO zur Sicherheitspolitik stellt klar, daß die Bedrohungen der Zukunft Cyberwar und Cybercrime heißen. Mein Neffe, seit über fünf Jahren erfolgreich im Internet unterwegs, hatte es mir bereits im Jahr zuvor gemeldet, daß kaum ein Tag vergeht, an dem nicht neue Angriffe entdeckt werden. Es droht der Zukunftskrieg auf der Datenautobahn.

Datenschleuder: *Können Sie die Bedrohungen konkretisieren, Herr Major?*

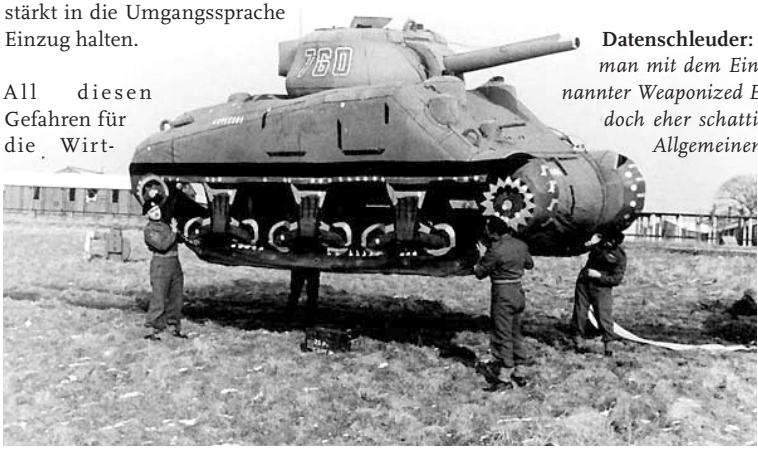
U. U.: Der internationale Terrorismus hält auch die Netze in Atem. Er beeinflußt unsere militärische Handlungsfähigkeit zunehmend durch Propaganda in Krisengebieten wie dem Hindukusch, in denen wir unsere Sicherheit verteidigen. Die kriegerischen Attacken auf unsere Infrastruktur bedrohen die militärischen und geheimdienstlichen Kommunikationskanäle. Und denken Sie auch an die Strom- und Wasserversorgung, alles durch diese Attacken bedroht,

denn jedes Computersystem kann von Digital-Terroristen gehackt und mit Datensprengsätzen angegriffen werden. Deswegen bauen wir in Zukunft vermehrt auf Vorwärtsverteidigungsviren statt nur konventionelle Bomben!

Datenschleuder: *Können Sie noch konkreter werden? Was droht uns und mit welchen Mitteln wird der Gegner zuschlagen?*

U. U.: Ich sage nur Stuxnet und Duqu! Glauben Sie denn, unsere Kernkraftwerke sind davor sicher? Und glauben Sie wirklich, der gemeine Zivilist könnte uns vor dieser neuen Bedrohung schützen?

Sie müssen verstehen: In unserem Cyberwar-Lagezentrum kann ich doch die Gefahrenlagen-Tafel jeden Tag sehen, die allgemeine Bedrohungs- und Überwachungslage hat sich seit Jahren nicht mehr aus dem tiefroten Bereich herausbewegt. Nicht weniger schlimm sieht es bei unseren Partnern im Pentagon aus. Und was mir allein mein Norton-Antivirus tagtäglich – ach, was sag ich? – stündlich! an erfolgreich abgewehrten Feindbewegungen meldet ... Wissen Sie, ich habe mir die deutsche Sprachanpassung des Programms von den Experten bei den Streitkräften anfertigen lassen – in Worten, die ich verstehe! Und um das richtige Gefühl für die feindliche Bedrohung auch in der Bevölkerung zu schärfen, muß dieses – wie ich finde, sehr präzise – Vokabular auch verstärkt in die Umgangssprache Einzug halten.



All diesen Gefahren für die Wirtschaft, Bevölkerung und Internetpornographie muß man doch qualifiziert begegnen!

Datenschleuder: *Was kann das Militär dagegen unternehmen?*

U. U.: Wir brauchen kleine, schlagkräftige Tiger-Teams, wahrscheinlich nach dem Geruch so benannte Raubtierkleingruppen aus fähigen Informatikern, die wir zusammenstellen werden, um zurückzuschlagen.

Diese werden wir mit dem Modernsten ausstatten, was die digitale Kriegsführung momentan anzubieten hat – und ich spreche hier nicht allein von Schulungen in, ich zitiere: „Kontrastrike“ und „Ketschur, the fläg“ – nein! Wir werden ein Arsenal an Even-Less-Than-Zero-Days, also Trojanerwurmviren, die erst übermorgen entwickelt werden, vom Netzwaffenmarkt einkaufen. Mittelfristig werden wir diesen Markt für unsere pro-aktiven Abwehrstrategien komplett leerkaufen, um dem Feind das Wasser abzugraben.

Besonders stolz sind wir hierbei auf einen schon 1995 testweise eingekauften Wurm, mit dem wir sämtliche im Umlauf befindliche Netscape Navigators im Handstreich unter unsere Kontrolle bringen können. Hiermit steht uns ein Untotennetzwerk umgedrehter feindlicher sogenannter Juser-Agenten ungeahnten Ausmaßes zur Verfügung!

Datenschleuder: *Aber unterstützt man mit dem Einkauf solcher sogenannter Weaponized Exploits nicht eine doch eher schattige Szene, die im Allgemeinen mit Internetkriminalität in Verbindung gebracht wird?*

U. U.: Sehen Sie, die Situation ist doch dieselbe wie mit der deutschen Schwerindustrie. Um

nicht unter den (von mir maßgeblich vorangetriebenen) Hackerparagraphen zu fallen, bleibt deutschen „Sicherheitsforschern“ inzwischen ja nichts anderes mehr übrig, als mit den autorisierten Verteidigungsorganen und deren zertifizierten und sicherheitsgeprüften Lieferanten zu kooperieren. Und unter uns: Für in ‚Tarngrün‘ gelieferten Code wird doch inzwischen deutlich mehr Geld gezahlt, als Jevgeni und Dmitri für ihre Banking-Trojaner je in die Hand nehmen könnten. Denn die Vorbereitung auf den dritten Weltkrieg in unseren Cyberkasernen können wir uns etwas kosten lassen.

Gut, die ersten zwei, dreimal ist nach dem Eingeben der Kreditkartennummer in dem per E-Mail bereitgestellten Formular nicht soviel passiert, außer daß von den lustigsten Orten ein paar krumme Beträge von unserem Konto abgebucht wurden. Dafür bekamen wir aber wenig später schöne Werbegeschenke mit unbekannten blauen Pillen, die wir mit Hilfe von ein paar als Leihgabe von der Bundeswehr gestellten Grundwehrdienstleistenden zu identifizieren versuchten. Außer von schmerzhaften Dauererektionen gibt es darüber jedoch nichts Außergewöhnliches zu berichten. Da wir uns über die Werbegeschenke sehr gefreut haben, nahmen wir diesen Lieferanten auch als ersten in unsere Freundesliste beim „De-Mail“-Programm auf.

Nachdem wir später dann ausschließlich über De-Mail kommunizierten, konnten wir sicher sein, daß die wenigen Firmen, die uns in dieser abgeschotteten Benutzergruppe Nachrichten zukommen lassen können, seriös sein müssen. Die hier angekauften Erstschlags-Exploits werden natürlich nach der Lieferung in gut gesicherten und von patroullierenden Cyber-Wachsoldaten bewachten Waffenkammern untergebracht. Die Ausbildungen zu php-Schutz-Ingenieuren laufen auf Hochtouren.

Datenschleuder: *Die zuletzt aufgetauchten Beispiele behördlicher deutscher Trojanerkunst gaben ja nun nicht sonderlich viel Anlaß zur Hoffnung ...*

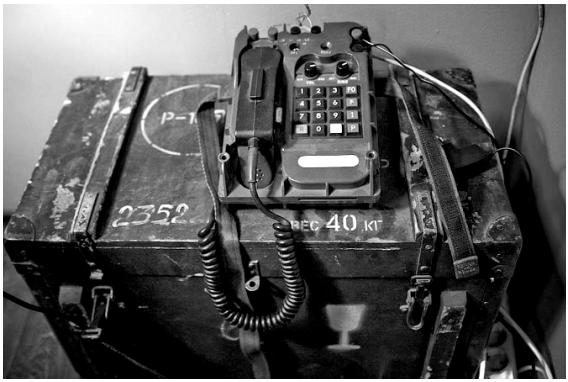
U. U.: Zumindest war die Sicherheitsüberprüfung des Zulieferes ta-del-los! Alle digital signierten Zertifikate lagen uns vor. Wir können uns nur schwerlich erklären, was hier schiefgehen konnte. Das müssen Sie unsere Kollegen bei den Polizeien fragen. Pannen solcher Natur kommen natürlich höchstens bei den Kriminalämtern, viel unwahrscheinlicher bei den Nachrichtendiensten und wirklich nie beim Militär vor.

Datenschleuder: *Von Netzfriedensaktivisten wird gern vorgebracht, daß das Internet eher ein Raum des friedlich-kooperativen Zusammenlebens und Teilens ist als ein Schlachtfeld ...*

U. U.: Hören Sie mal! Was ein Schlachtfeld ist, bestimmt ja wohl immernoch das Militär! Churchill hätte sich gewiß auch nie träumen lassen, daß Coventry zum militärisch-strategischen Einsatzziel aufgewertet werden würde. Genauso, wie die Wirtschaft jüngst den ungewaschenen langhaarigen Hippies das Internet streitig machen konnte, wird zwangsläufig auch das Militär zum Schaffen von Ordnung und zur Sicherung der virtuellen Grenzen Einzug halten.

Das Internet ist ja schon von der Struktur her sehr diszipliniert und hierarchisch angelegt! Ganz oben kann man aus Google-Internet-Lageplänen den Tagesbesuchsplan für Internetseiten zusammenstellen, dann kommt man von Google aus ja auch zu Facebook, wo man wiederum Truppenstärke und -zustand für befreundete Verbände meldet. Und nebenan bei Twitter gibt es immer hochaktuelle Meldungen von den zivilen Streitkräften. Einzig in Terrorraubkopier-Freischärlernetzen herrschen noch chaotische Zustände. Das nennt sich neumodisch „Peer-to-Peer“ und heißt auf deutsch, daß da jeder mit jedem spricht! Keinerlei Funkdisziplin. Hier wird offenbar, daß ohne die ordnende Kraft des Militärs ständig das Faustrecht und bürgerkriegsähnliche Zustände ausbrechen.

Sehen Sie, so ein im Internet gewonnener Krieg macht sich in den Abendnachrichten doch viel schöner, das müssen doch auch die Friedenstauben begreifen! Wer will schon Bilder von durch Granaten zerfetzten Kindern sehen, die sich im eigenen Blute suhlen und deren Gedärm... Entschuldigung, ich schweife ab. Können denn



diese in ihrer Blümchenwiesen-Phantasiewelt verhafteten Nerds mit ihrem Gewissen vereinbaren, daß die Armeen sich weiter in der realen Welt blutige Gefechte liefern? Ich denke nicht!

Bilder von demotivierten und geschlagenen Gruppen feindlicher Computerkrieger kann man leicht durch im Netz verfügbare Fotos von LAN-Parties visualisieren. Der Trend geht doch schon seit Jahren zum grünstichigen Bild, auf dem man Bomben quasi wie im Killerspiel aus der eigenen Perspektive beim Zerstören von ein paar hilflos herumflitzenden Bildpunkten auf dem Boden verfolgen kann. Wäre es nicht viel schöner, wenn dies einfach nur Computergegner sein könnten?

Datenschleuder: *Wie definieren Sie in diesen „Kriegs"-szenarien den Feind?*

U. U.: Dazu muß man doch erst einmal festhalten, wer überhaupt angefangen hat! Meines Erachtens war doch schon Rick Astley ein feiger kriegerischer Angriffsakt, der nicht unvergolten bleiben kann.

Und auch die Mengen feindlich-negativer Propaganda, die aus unkontrollierten Rechenzentren der gesamten Welt auf unsere Bevölkerung eintrommeln, sollten uns nachdenklich stimmen. Hier benötigen wir dringend Erstschlagskapazität! Diese müßten wir natürlich zuerst an eigener Infrastruktur testen. Der Vorschlag des Notaus-Knopfs für das Deutsche Internet kann dabei doch nur ein zukunftsweisendes Beispiel sein. Ein paar Katastrophen- und Alarmübungen sind natürlich ebenso unerläßlich. Zweifelsohne müssen auch Tricks und Kniffe aus der konventionellen Kriegsführung im Internet Einzug halten. Eine abendliche Verdunklung ab 1800 wird ja beispielsweise schon von einigen Sparkassen erfolgreich erprobt.

Und ob nun Chinesen auf Bundesregierungscomputern Spionagebrückenköpfe einrichten oder dies eher israelische Militär-zero-overload-forces über Chinaproxies sind, spielt ja für die Legitimierung eines NATO-Abwehrzentrums erstmal keine Rolle.

Datenschleuder: *Aber besteht denn bei Vergeltungshandlungen gegen Akte unbekannter Urheber nicht die Gefahr exponentieller militärischer Eskalation, die sich im Zweifel auch wieder durch Militärschläge in der realen Welt manifestiert?*

U. U.: Wundervoll, nicht wahr? Genau dies ist doch die asymmetrische Kriegsführung, mit der konventionelle Armeen in den letzten Jahrzehnten genug Erfahrungen sammeln konnten. Wer sonst sollte sich denn bitteschön damit auskennen?

Und unter vier Augen: Ein bißchen Kollateralschwund ist doch immer. *(kichert jovial)*

Datenschleuder: *Ist denn ein Ende eines solchen kybernetischen Krieges überhaupt vorstellbar?*

U. U.: Nein! Und gerade das ist doch das Schöne! Man erinnere sich nur, welche wundervollen technischen Neuerungen alleine das Wettrüsten während des Kalten Krieges hervorgebracht hat. Und auch nach der erfolgreichen Niederschlagung des Feindes aus dem Kalten Krieg hat die NATO einen ungeheuren Erfahrungsschatz gesammelt, der durch einen plötzlichen Frieden nur unnötig gefährdet würde.

Datenschleuder: *Herr Major, wir danken Ihnen für das Gespräch und Ihre entwaffnende Offenheit.*