Ingo Ruhmann:

Cyber War: Will it define the Limits to IT Security?

Abstract:

Cyber warfare exploits the weaknesses in safety and security of IT systems and infrastructures for political and military purposes. Today, not only have various units in the military and secret services become known to engage in attacks on adversary's IT systems, but even a number of cyber attacks conducted by these units have been identified. Most cyber warfare doctrines aim at a very broad range of potential adversaries, including civilians and allies, thus justifying the involvement of cyber warfare units in various IT security scenarios of non-military origin. Equating IT security with cyber warfare has serious consequences for the civil information society.

Agenda:

Author:

Ingo Ruhmann

- Fachhochschule Brandenburg, Security Management, Magdeburger Str. 50, 14770 Brandenburg an der Havel, Germany
- Email: ruhmann@fh-brandenburg.de, Web: http://www.fh-brandenburg.de/~ruhmann/index.html
- Relevent Publications:
  - Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs; Dossier Nr. 72, in: **Wissenschaft und Frieden**, Heft 1, 2014, S. 1-16
  - Ingo Ruhmann: NSA, IT-Sicherheit und die Folgen. Eine Schadensanalyse; in: **Datenschutz und Datensicherheit** (DuD), Heft 1, 2014, S. 40-46
  - J · gen Altmann, Ute Bernhardt, Kathryn Nixdorff, Ingo Ruhmann, Dieter W · rle: Naturwissenschaft – Rüstung - Frieden. Basiswissen für die Friedensforschung. Reihe Friedens- und Konfliktforschung, Band 9. VS-Verlag, Wiesbaden, 2007
  - Ingo Ruhmann: Cyber-Terrorismus. Panikmache oder reale Gefahr? In: Ulrike Kronfeld-Goharani (Hg.): **Friedensbedrohung Terrorismus**. Ursachen, Folgen und Gegenstrategien. Kieler Schriften zur Friedenswissenschaft, Band 13, Kiel, 2005, S. 222-240
  - Ute Bernhardt; Ingo Ruhmann: On Facts and Fictions of „Information Warfare" In: Bernhelm Boos-Bavnbek, Jens Hoyrup (Eds.): **Mathematics and War**, Basel, 2003, S. 258-282
  - Ingo Ruhmann, Christiane Schulzki-Haddouti: Kryptodebatten. Der Kampf um die Informationshoheit; in: Christiane Schulzki-Haddouti (Hg.): **B · gerrechte im Netz**, Bundeszentrale für politische Bildung, Bonn, 2003, S. 162-177
  - Manuel Kiper; Ingo Ruhmann: Überwachung der Telekommunikation; in: **Datenschutz und Datensicherheit** (DuD), Nr. 3, 1998, S. 155-161
  - Ute Bernhardt; Ingo Ruhmann: Der digitale Feldherrnhügel. Military Systems: Informationstechnik für Führung und Kontrolle. Dossier Nr. 24, in: **Wissenschaft und Frieden**, Heft 1/97, S. 1-16

ISSN 1614-1687

The diffusion of computer malware such as viruses, worms and trojans today is a commonplace peril of computer use. Disrupting digital computers and modifying data stored in IT systems has been practiced since the late 1970s. Since the mid-1980s, the military and various intelligence services in both east and west have experimented with data espionage[1] and computer sabotage directed against IT systems as a seemingly useful tactic from a military and technological perspective[2]. Disruptions of IT systems for propaganda purposes between conflicting groups, states or non-state-actors have been recorded at least since 1995[3].

Since the early 1990s, various countries have developed conventional warfare doctrines based on IT systems and have since built up military resources for cyber defense and offense. As a common term for this broad use of manipulation of IT systems and data in military contexts, "information warfare" was coined that integrates all operations that relate to command and control of forces and the data and intelligence necessary for it.

- Information warfare is operationalised as "information operations" that encompass all "information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries"[4]. This is not only applied to military contexts, where information operations aim at the disruption and sabotage of an adversaries' command and control system, but explicitly also to non-military contexts[5]. Information warfare ranges deep into the intelligence area, psychological warfare and media manipulation while on the other side it encompasses an extremely intensified conventional warfare and at its maximum the use of EMP generators, if necessary, even by nuclear devices[6].
- The term "cyber warfare" – which is not defined as a military term[7] - is used for operations below the level of physical or conventional military operations, mostly as a synonym for a disruptive use of manipulation tools in computer networks. Cyber warfare is described especially as a tool in low-intensity,

[1] Klaus Koch, who was charged with selling stolen data to the KGB and in 1989 was found dead near Hannover, was an early example for intelligence units acquiring knowledgeable private parties for their purposes, see: http://www.heise.de/ix/artikel/Suendenfall-794636.html

[2] U.S. agencies admitted to physically access computer systems situated behind the former iron curtain in the 1970s and '80s, see: Jay Peterzell: Spying and Sabotage by Computer. Time, March 20, 1989, S. 41

[3] Defacements were not gleaned and documented before 1995, when the IT security web site attrition.org started recording them. The site stopped doing so in 2001 because of an exponentially growing number of incidents, see: http://attrition.org/news/content/01-05-21.001.html

[4] U.S. Department of Defense: Field Manual 1-02, Operational Terms and Graphics, Sept. 2013, p. 1-99, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp1_02.pdf

[5] One of the most complete military doctrines publicly articulated is the 2003 version of the U.S. Army Field Manual 3-13 "Information Operations: Doctrine, Tactics, Techniques, and Procedures", Washington, November 2003, http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf . This comprehensive view has since been superseded by several Field Manuals detailing different aspects of information warfare.

[6] Explicitly demanded as an option in the Gulf War 1991, see: John Barry: The Nuclear Option: Thinking the Unthinkable; in: Newsweek, 14.01.91, S. 12-13. Today the U.S. think tank Center for Security Policy campaigns against the dangers of a nuclear-device triggered EMP: http://www.centerforsecuritypolicy.org/category/homeland-security/infrastructure-and-emp/

[7] The NATO's Tallinn Manual uses the term cyber warfare "only in a purely descriptive, non-normative sense": Michael N. Schmitt (Ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge, 2013, p. 4, Footnote 17. The DoD does not define cyber warfare at all: see the DoD's definitions of military terms in Field Manual 1-02, Operational Terms and Graphics, Sept. 2013, (http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp1_02.pdf) and the Memorandum by the Vice Chairman of the Joint Chiefs of Staff: Joint Terminology for Cyberspace Operations, Washington, Nov., 2010, http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf

ISSN 1614-1687

often asymmetrical conflicts[8]. It is differentiated in most armed forces into defensive measures – computer network defense, or "counter-cyber"[9] – and offensive activities. The most specific act is a "cyber attack" defined to be carried out by computer against IT systems[10].

Information warfare thus includes all operations directed against all coordinating structures of an adversary – by now mostly IT-based - while at the same time improving one's own capabilities in coordinated fight under extensive command and control. In this perspective it is consistent to see any kind of information processing as a target – irrespective of this being done on technical systems or by humans. For these targets to be identified and hit, it is also necessary to collect all data available at all times. Cyber or information operations from a military point of view are a modern extension of electronic warfare that has been waged continuously since the end of World War II. Data on the specifics of any potentially relevant electronic system have been collected and stored to be used in combat. Like electronic warfare, information operations thus are explicitly defined to extend the scope of military activities far beyond armed conflict deep into the intelligence realm. Information operations will therefore always encompass activities on civilian infrastructures. This is reflected by organizational structures: In most countries, information and signals intelligence is gained by special organizations combining armed forces and intelligence services that now regularly form combined information warfare units.

The classic use of all these data – in military terms - are "Advance Force Operations" that prepare for the main strike by seizing "supporting positions – including key network systems or nodes – pre-emplacement or clearing of weapons – such as […] preliminary bombardment […] , or cyber access and / or weapon implants"[11]. So in contrast to electronic warfare, information operations are not only seen on a purely symbolic and digital level, but always with a "physical dimension"[12] including "the elimination of targeted enemy systems. […] Various weapons and techniques — ranging from conventional munitions and directed-energy weapons to network attacks — can destroy enemy systems that use the electromagnetic spectrum"[13].

From this perspective, it should be clear that information operations always combine two properties: at first, a permanent "state of war" waged in clandestine theaters extending the scope of military activities deep into the civilian realm and second, the use of physical access and conventional force as a tool and a desired effect. Unlike electronic warfare, consisting of mostly passive intelligence gathering – although in fact it came with regular intrusions into enemy territory and quite a number of armed engagements leading to the loss of servicemen[14] -, information warfare consists of attack and sabotage of IT systems, disrupting vital infrastructures and potentially leading to widespread and catastrophic breakdowns, when for example a nation's power grid is targeted. The "9/11" terrorist attack resulted in the invocation of Article 5 of the NATO Alliance considering this deed as an armed attack against all members. Information warfare against critical infrastructures will likely produce fatal consequences of an even worse scale, extending the concept of warfare with lethal consequences into the digital domain.

[8] See for example: Samuel Liles: Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency; Conference on Cyber Conflict, NATO CCD COE Publications, 2010, p. 47-57

[9] Vice Chairman of the Joint Chiefs of Staff: Memorandum: Joint Terminology for Cyberspace Operations, Washington, Nov., 2010, http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf , p. 4

[10] Vice Chairman of the Joint Chiefs of Staff: Memorandum: Joint Terminology for Cyberspace Operations, Washington, Nov., 2010, loc. cit., p. 5

[11] Vice Chairman of the Joint Chiefs of Staff: Memorandum: Joint Terminology for Cyberspace Operations, Washington, Nov., 2010, loc. cit., p.2

[12] U.S. Department of Defense: Field Manual 3-13. Inform and Influence Activities, Jan. 2013, p. 2-2

[13] U.S. Department of Defense: Field Manual 3-36, Electronic Warfare, Nov. 2012, p. 1-11

[14] Between 1950 and 1959 alone, of the U.S. signals intelligence airplanes entering the airspace of "communist states" to elicitate reactions, 33 were shot down, killing almost all the servicemen onboard. See James Bamford: The Puzzle Palace. Inside the National Security Agency - America's Most Secret Intelligence Organization. Harmondsworth, S. 239

IT Security and Cyber Warfare

The concentration on cyber warfare seen in the last years has led to a fundamental change in the reception and interpretation of classic computer crime committed by civilian actors, the role of law enforcement vs. the military in computer crime and IT security, the solution of inter-state conflict by diplomatic or non-peaceful means and even the co-operation between formal allies in the political and economic arena.

One of the central aspects of cyber warfare remains the attribution of an IT security incident to its origin and the assessment, whether it might be a military act or not. Attackers may be experimenting youths, professional hackers or attackers in the military or intelligence services.

The evolution of IT system manipulation over the last 40 years has produced a booming IT security industry dedicated to keeping hacking incidents and malware proliferation at bay. Although the exploitation of IT security deficits and the development of countermeasures displays some facets of an arms race, a commercial calculation pervades on all sides of this development as a baseline:

- Non-commercial experimenting hackers on the one hand seek attack paths on any technology level, but mostly do little damage.
- Cyber criminals interested in financial rewards on the other focus on profitable and widely applicable schemes and techniques.
- IT security companies develop countermeasures against the most commonplace and – assessing potential damages – urgent security breaches.

This has led to some kind of security equilibrium, where the number of cybercrimes has grown exponentially according to the incident statistics, while the overall share of infected IT systems compared against the deployed technology base as a whole has shown no marked increase[15] – although one should be aware that none of the statistics stands close examination[16].

Computer scientists and the IT industry have supported the containment of malware production and distribution on the one hand by improving and implementing software development methods and on the other by a speedier reaction when a security problem emerges. From an understanding of professional ethics[17] coupled with the need to keep customers' trust, many hackers, IT security professionals and software vendors have established ways and incentives to exchange knowledge on newfound problems before others exploit or publish them. This kind of self-regulation has made hacking an unpredictable way of testing for security holes and a step in IT product improvement.

Somewhat lagging is the engagement of the civil law enforcement agencies. Around the world, it has taken years for existing laws on cybercrime to be applied. In the 1990s, only some dozen cybercrime cases per year

[15] Microsoft as the biggest operating system vendor tracks infections encountered and removed by its malware removal software. While "encounters" with malware are common, the world wide average of computers cleaned in the last 10 years was given constantly at around 1.2 per cent: Microsoft Security Intelligence Report: Special Edition 10 Year Review, p. 30; http://www.microsoft.com/en-us/download/details.aspx?id=29046. In 2013, 17 per cent of PCs with a Microsoft operating system worldwide "encountered" malware, but only 0.6 per cent were actually infected: Microsoft Security Intelligence Report. Worldwide Threat Assessment, Vol. 15, Jan-June 2013, p.27, http://download.microsoft.com/download/5/0/3/50310CCE-8AF5-4FB4-83E2-03F1DA92F33C/Microsoft_Security_Intelligence_Report_Volume_15_Worldwide_Threat_Assessment_English.pdf

[16] Microsoft researchers analyzed cybercrime surveys available with the result that "they are so compromised and biased that no faith whatever can be placed in their findings": Dinei Florencio, Cormac Herley: Sex, Lies and Cyber-crime Surveys, Redmont, Juni 2011, S. 8; http://research.microsoft.com/apps/pubs/default.aspx?id=149886 and http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf

[17] See especially the ACM Code of Ethics: http://www.acm.org/about/code-of-ethics

were recorded[18]. Even today, the statistics reveal a huge gap between actual cybercrime cases and law enforcement activities[19], the reason of which can only be seen in the small number of enforcement personnel. This deficit leaves many cybercrimes unpunished.

The problems of attribution of cyber crimes and the lack of criminal prosecution on the one hand and the very broad view of information warfare stretching far into the civilian space on the other has led to a differentiated analysis of cyber activities and potential military reactions. A group of experts invited by the NATO Cooperative Cyber Defense Centre of Excellence developed a detailed assessment of cyber attacks regardless of the originator and a corresponding escalation sequence including the use of physical force deemed legal under international law[20]. The so-called "Tallinn Manual" tries to develop some kind of decision tree for the onset and justification of military operations in cyberspace. The Manual is an elaborate document on the level of operations in Cyberspace that start with purely civilian participants and may escalate into armed conflict.

A reason for the deficits in criminal prosecution and for a potential role for the military is seen in the international character of computer misuse: Attackers routinely employ vulnerable IT systems anywhere on the Internet to stage malicious activities to mask their origin, the goal of their attack and to disrupt investigative work.

As a civil remedy, the Council of Europe in 2001 concluded a Cyber Crime Convention to enable a quick international cooperation of civilian cybercrime units[21]. The Convention however does not call for cooperation, when security interests of one party are concerned[22] – for example if an espionage agency of one of the countries is participating in an incident. Although this is consistent with the total lack of international regulations of espionage activities, this however is a severe disadvantage when IT security incidents become more and more part of espionage operations.

While governments worldwide are securing cyberspace by different means[23] the limited effects of law enforcement however, are used explicitly in the U.S. as an argument to involve other private and non-civilian players and to introduce the idea of cyber deterrence as a goal:

> *"To date, the U.S. Government has been implementing traditional approaches to the cybersecurity problem—and these measures have not achieved the level of security needed. This Initiative is aimed at building an approach to cyber defense strategy that deters interference and attack in cyberspace by improving*

---

[18] In the U.S., data on internet-related fraud were collected since 2000. The first report showed 49.711 complaints, 80 per cent of them consisting of auction fraud, "Nigerian Letter fraud", and the rest of other forms of fraud. Malware-based fraud was hardly given as a reason for complaints: The Internet Fraud Complaint Center. 2001 Internet Fraud Report, p.3, http://www.ic3.gov/media/annualreport/2001_IFCCReport.pdf . This is comparable to other countries: Conventional credit card fraud, subsumed under computer crimes is the only category with a high number of cases in many statistics (stated explicitly in: Polizeiliche Kriminalstatistik p. 15, footnote 1). By comparison the number of computer-related crimes was given a) computer sabotage with 302 cases (p. 42), and b) data espionage with 210 cases (sp. 43); see: Bundeskriminalamt: Polizeiliche Kriminalstatistik, Wiesbaden, 1999, www.bka.de/nn_242508/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/pksJahrbuecherBis2011/pks1999,templateId=raw,property=publicationFile.pdf/pks1999.pdf

19 Comparing available data, in 2009 three trojans were responsible for the infection of 400,000 computers in Germany (http://www.microsoft.com/de-de/download/details.aspx?id=11722). For the same period, only 2,200 cases of computer sabotage of any kind (§303a StGB) were reported in the statistics of law enforcement agencies. So, 0.5 per cent of the known trojan malware cases were reported, 99,5 per cent went unreported, see: BMI: Polizeiliche Kriminalstatistik 2009, S. 44; http://www.bmi.bund.de/cae/servlet/contentblob/1069004/publicationFile/65239/PKS2009.pdf

[20] Michael N. Schmitt (Ed.): The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge, 2013

[21] Convention on Cybercrime CETS No.: 185 has since been ratified by 41 and signed by further 11 countries, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

[22] By Article 27 Nr 4 b) of the Convention cooperation requests may be refused, if one party "considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests".

[23] The German Federal Government for example states that cyber attacks can have a criminal, terrorist, espionage or military background and seeks to enhance cyber security under civilian guidance: Bundesministerium des Inneren: Cyber-Sicherheitsstrategie für Deutschland, Berlin, Feb. 2011, S. 3f; http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

warning capabilities, articulating roles for private sector and international partners, and developing appropriate responses for both state and non-state actors"[24].

State Actors as Cyber Warriors

Non-civilian actors in cyber security have a profound effect on the equation of IT security as a whole. The alarm sounded by McAfee about the "Age of cyber warfare" being here, points to this threat to the status quo in IT security: State actors have a markedly different set of reasons for the development and application of malware as well as the ability to muster resources vastly exceeding those of even the largest cybercrime organization.

No government organization publicly had claimed the credit for cyber sabotage of other nation's computer installations until details of the U.S. Government operation "Olympic Games" dating back to President George W. Bush and continued by Obama were reported[25]. NSA and Israeli specialists programmed a trojan they called "The Bug", used in different versions in Iran. When it appeared on computers worldwide after some modifications, it became known under the name of "Stuxnet", targeting Siemens industrial IT systems[26]. Since then, several incidents were traced back to originators in other countries and were deemed to be a targeted cyber warfare attack. In the last years, cyber warfare has become a synonym for a number of IT security incidents with various targets and originators[27].

The analysis of Stuxnet showed the extreme efforts undertaken. "Duqu", that shares significant parts of code with Stuxnet, even showed fingerprints of a hitherto unknown programming language. Connected to Stuxnet and its trojan siblings Wiper and Duqu, "different platforms used to develop multiple cyber-weapons" were identified, named Flame[28], Tilded and Gauss[29]. The technical analysis shows very strong evidence that Stuxnet and its siblings all originated from the same source although U.S. authorities only were connected to Stuxnet and Flame[30].

The investments of "a substantial amount of time and money to build such a complex attack tool"[31] with these specialized technical abilities can hardly be matched by commercial IT security endeavors[32], resulting, as in the

---

[24] see: National Security Council: The Comprehensive National Cybersecurity Initiative (unclassified), Washington, March 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[25] David E. Sanger: Obama Order Sped Up Wave of Cyberattacks Against Iran; New York Times, June 1, 2012, p. A1; http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[26] Two open questions on Stuxnet are, a) how the highly specialized knowledge of Siemens industry control systems was acquired to develop Stuxnet and to what extent Siemens was compromised and, b) how the trojan infection with an USB memory stick was executed at the isolated uranium enrichment site in Iran, although this procedure of physical access is already known to be used by U.S. agencies.

[27] In 2009, the IT security company McAfee claimed for the first time, that government operations and cyber war had become a major problem in IT security; see: McAfee: Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare, Santa Clara, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF

[28] Flame was said to predate Stuxnet and was detected after infecting oil processing installations based on activities by Israel, see: Ellen Nakashima, Greg Miller, Julie Tate: U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say; in: The Washington Post, 19.06.2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

[29] Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected, June 11, 2012, http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected

[30] See Alexaner Gostev: Kaspersky Security Bulletin 2012. Cyber Weapons, http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons.

[31] Executive Director of ENISA, Dr Udo Helmbrecht in a Press Statement EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection; http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1

[32] The conclusion of IT security experts: "The takeaway is that nation-states are spending millions of dollars of development for these types of cybertools, and this is a trend that will simply increase in the future"; see: David Kushner: The Real Story of Stuxnet; IEEE Spectrum, 26 Feb 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

case of Stuxnet and Duqu, in an extended period of unnoticed pervasion. While Stuxnet infected industry systems, its sibling trojans and platforms infected 350.000 IT systems in commerce, banking, and private IT systems the Middle East alone[33].

The origins of these attacks came into the open in 2013. The revelations about the U.S. National Security Agency (NSA) activities against Internet users in the media were mostly concentrated on surveillance aspects – referenced by the code names "PRISM" and "XKeyScore"[34]. It showed the extensive character of intelligence gathering on networked communication that only seems limited by technical factors. But no less important is NSA's role in information warfare: The NSA – unlike the CIA – is a part of the military command hierarchy, the agency's director being the supreme commander of the U.S. Cyber Command heading information operations units in all four armed services – Army, Air Force, Navy and Marine Corps –, "responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations"[35].

In the media it almost went unnoticed that XKeyScore does not only track communications metadata and several days of Internet traffic content. XKeyScore – the successor to a number of more or less successful software developments in the last 15 years to collect, analyze and manipulate Internet traffic[36] - is one of several dozen known "digital network intelligence" tools used by NSA today. It is also used as an automated "cyber operations" tool collecting data on the type and specific details of IT systems, scanning targeted systems automatically for typical vulnerabilities taken from specialized data bases[37]. In selected cases, an automatic malware infection is being applied through XKeyScore.

Responsible for the development of the automated tools and targeted attacks is the "Office of Tailored Access Operations" (TAO), part of the SIGINT branch of NSA[38]. Since 1998, the about 600 TAO officers have been hacking into IT systems either by remotely inserting malware or by ordering intelligence operatives at the targeted destination to physically access and manipulate computers in so-called "off-net operations," – thus employing the same operative tactics of physical access as developed and employed in the 1970s[39].

Although the total amount of attacks by TAO is unknown, NSA conducted 231 targeted offensive cyber operations in 2011 alone, infecting tens of thousands of computers and aiming to expand this to millions of systems[40]. This does not include infections of IT systems in government, banks and companies in the Middle East with Stuxnet and its malware siblings.

The financial resources of NSA and its British counterpart GCHQ used to gather intelligence, develop and apply cyber warfare software and stage attacks are orders of magnitude higher when compared to cyber criminals

[33] Alexander Gostev: Kaspersky Security Bulletin 2012. Cyber Weapons, loc. cit. Banking and commerce, as we know by now, are a prime NSA target in EU countries as well. The number of infections should be compared to the Microsoft account of conventionally infected IT systems in German in 2009 which was only slightly higher – see footnote 18

[34] See especially the voluminous documentation and compilation of material by The Guardian: http://www.theguardian.com/world/nsa

[35] Mission Statement of the U.S. Cyber Command, http://www.stratcom.mil/factsheets/Cyber_Command/

[36] See the reports on the Congressional debate on the estimated 2 billion Dollar costs of NSA systems developed 2005 – 2007, most notably the discontinued "Trailblazer" for massive data collection and "Turbulence" for the selective control of Internet nodes, web traffic surveillance and selective data packet modification: Siobhan Gorman: Costly NSA initiative has a shaky takeoff, Baltimore Sun, Feb. 11, 2007, http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa

[37] Konrad Lischka, Christian Stöcker: NSA-System XKeyscore: Die Infrastruktur der totalen Überwachung; Spiegel Online, 31.07.2013; http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html;

[38] Matthew M. Aid: Inside the NSA's Ultra-Secret China Hacking Group; in: Foreign Policy, 10. Juni, 2013; http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group?page=0,1

[39] Matthew M. Aid, loc. cit. for TAO, Jay Peterzell, loc. cit. for activities since the 1970s.

[40] Barton Gellman, Ellen Nakashima: U.S. Spy agencies mounted 231 offensive cyber operations in 2011, documents show; in: Washington Post, 31. Aug. 2013; http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration

and of course private hackers. NSA invests 2 billion US Dollars in a massive data center alone[41], $652 millions over the last years on "covert implants" software[42], and – with industry partners – additional billions in IT security development[43] – which, as we can deduce from the knowledge of past developments, will result in additional surveillance and cyber attack technology.

Compared to other nations, the organizational structure of NSA and Cyber Command in the U.S. and its counterparts in the U.K., Canada and other allies is rather common. The German Bundeswehr also has concentrated all of its intelligence gathering assets, electronic, psychological and information warfare capabilities in the "Kommando Strategische Aufklärung" (KSA, Strategic Intelligence Command) employing roughly 6.000 soldiers[44].

These revelations by the media and professional analysis clearly show that cyber warfare attacks by state actors meanwhile play a very significant role in IT security globally.

Down the Road to cyber warfare

Taking all the facts together and connecting the dots, we can sketch a picture of hardly limited surveillance, intelligence collection and IT system manipulation from the 1970s on. New algorithms allow the massive expansion of technical capabilities with the goal, as stated by NSA director Alexander, to simply collect and analyze all data accessible. Results from these vast amounts of data are targeted attack paths on IT systems that have been collected in data bases and used since the end of the 1990s. The NSA is by no means the only actor in this game. Others – like Russia's FSB and China – are following suit, but are clearly lacking the same amount of technology and resources.

By the already classic definition of actors in cyber warfare as "anyone with the capability, technology, opportunity, and intent to do harm"[45] this kind of warfare is thoroughly asymmetrical. NATO's Tallinn Manual extensively elaborates the point of isolated individuals that can disrupt vital infrastructures of a nation resulting in severe damages and even loss of life. The Manual then specifies operational attributes that may allow counter-attacks in cyberspace as well as physical military operations in the real world.
"Anyone" as an originator of IT security incidents might be valid as a description of a very broad type of actors. However, "anyone" is not valid seen from the perspective of a civilian assessment of computer crime as a percentage of IT usage. Although IT security incidents are rising continuously, the annual reports of major IT security companies show that only between 0.03 and 3 per cent of computers are infected. Although extremely understaffed, civilian computer crime policing, together with IT security companies and IT professionals, have for the last decades successfully prevented any IT security catastrophe.

"Anyone" as an actor in IT security incidents on the other hand, is an extremely broad category as a basis for military operations that are under international law nearly exclusively restricted to hostilities between states. Operations directed against individuals like terrorists or criminals are still seen as the field of criminal prosecution. It can nowhere be seen, that the military is better able at defeating computer crime or prosecuting criminals than a civilian police force.

---

[41] James Bamford: The NSA Is Building the Country's Biggest Spy Center (Watch What You Say); in: Wired. 15.03.2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

[42] Gellman, Nakshima: U.S. Spy agencies mounted 231 offensive cyber operations in 2011, documents show; in: Washington Post, loc. cit.

[43] Tom Simonite: Digitale Geister, die ich rief; in: Technology Review, 02.03.2012, http://www.heise.de/tr/artikel/Digitale-Geister-die-ich-rief-1446457.html

[44] http://www.kommando.streitkraeftebasis.de/portal/poc/kdoskb?uri=ci%3Abw.skb_kdo.ksa.ksa

[45] The President's Commission for Critical Infrastructures Protection, Washington, 1997, documented at: http://www.iwar.org.uk/cip/resources/pccip/backgrd.html

"Anyone" as a potential adversary of "cyber warriors" is not only the consequence of the surveillance practiced by NSA and others. It is routine for IT security. The military originators of Stuxnet have proven this point: Stuxnet has circulated way beyond its original destination and infected numerous IT systems. Computer malware cannot be controlled – exactly as a dangerous pathogen in biological warfare. In IT security, cyber warriors are waging war against every IT user through the application of indiscriminate tools and – vastly more important - the weakening of IT security.

The past has shown that a common interest of IT professionals as a community lies in the reduction of vulnerabilities and in minimizing the unreliability of IT systems. Sound software development should be employed widely. But most importantly, the established, but fragile civilian way to diminish existing IT security risks now becomes an imperative in the professional ethic of IT personnel. The ethically sound answer from a professional point of view may sound strange: Extensive testing for IT security holes by hackers – including even the support of these activities by the IT industry – and bringing IT system vendors to quickly produce patches for the security-related results found mutates into a civilian safeguard process against cyber operations by forces way beyond the abilities of civilian actors. This course of action and further security measures have to be stepped up. Although the call for intensified civilian hacking as a permanent test instance against backdoors and security problems is in fact a weird solution, it is an act of necessity within the IT profession against the corruption of IT security by state actors and the lack of criminal prosecution of these and other cyber delinquents that often are even protected by law.

In the last years, we have seen a succession of steps to move IT security problems from the civilian into the military domain:

- The civilian resources on cybercrime always were and still are severely limited compared to their military counterparts.
- International co-operation against cybercrime is exempted when military or secret services, their subcontractors or their proxies are involved. The more IT security incidents become a part of espionage operations, the less value any improved international effort against cybercrime will probably have. This limitation is used as an argument by military actors for their growing share of cyber warfare responsibilities for non-civilian actors.
- Military and secret services in different countries have legal access to IT systems and IT technology well beyond the access granted to criminal investigators under the rule of law. These services not only used special knowledge to fabricate faked IT security credentials in Stuxnet. It is known since the 1990s, that they influence companies to keep back doors as hidden access points[46].
- Military and secret services have collected intelligence data for decades on an extremely vast scope to actively pursue cyber warfare not only against assumed enemies, but even allies[47].

In short: There not only is no safeguard against military and secret services as the most resourceful actors by far in compromising IT security. This lack is even used as an argument to push back even further civil criminal prosecution responsibilities in cybercrime. Cyber warfare that equates IT security incidents with clandestine sabotage activities by secret services and the proxies they employ, is supported by laws that force IT companies into co-operation to undermine a broad range of technological safeguards against breaches of IT security, and in the end opening up manipulation paths for cyber criminals and others. There is no legal way to operate secure mail or trusted cloud services in the U.S. without allowing authorities access to the data[48]. This has also

[46] Duncy Campbell: How NSA access was built into Windows; Telepolis, 4.09.1999, http://www.heise.de/tp/artikel/5/5263/1.html

[47] The CERT of the German Bundeswehr has stated for year that it fights not only terrorists and adversaries, but also friendly intelligence services, see slide 3 of: http://www.afcea.de/fileadmin/downloads/Young_AFCEAns_Meetings/20090216%20Wildstacke.pdf

[48] Which is why the two companies Lavabit and Silent Circle closed their operations altogether. See: Jürgen Schmidt: Todesurteil für Verschlüsselung in den USA; Heise Security, 4.10.2013, http://www.heise.de/security/artikel/Todesurteil-fuer-Verschluesselung-in-den-USA-1972561.html

been seen with the producers of crypto systems[49]. Even Microsoft had to change its software after noticing that the Flame trojan spread through faked digital security IDs[50].

The more cyber warfare is used as espionage and sabotage tools of state actors against "anyone", the less chance there is to reach an international agreement or even just a co-operation amongst allies, since espionage for obvious reasons has never been regulated internationally.

A no holds barred cyber warfare amongst enemies and allies alike, as currently seen, thus is an even riskier development to peace, international stability and the civil society than the previous establishment of information warfare as a military doctrine confined to theaters of armed conflict.

From the ethics of IT professionals it follows that they are in demand on a broader level. IT professionals are the most knowledgeable in assessing and communicating the consequences of restricted IT security resulting in severe security and safety risks in the civilian – but also military – IT infrastructure. The risks are not restricted to the digital world. The discussion of the NSA scandal has shown the relationship between a mobile phone number acquired and a lethal drone strike[51]. Cyber operations can have immediate consequences for everyone just when one considers the implications of IT security holes left unpatched combined with a military reaction on their exploitation that may result in military actions taken. The expertise of IT professionals is in demand if there is to be a chance for political control of information warfare.

The result of broad surveillance ultimately is the end to free society. A debate on this development is urgently needed. However, the result of a purposeful manipulated and weakened IT security infrastructure runs deeper: If a digital identity cannot be trusted, or IT systems in industrial plants run out of control because a Stuxnet-like malware causes catastrophic disasters, the result is the loss of control over the digital world we today rely on and even try to extend into an "Internet of Things" surrounding us. Manipulating, weakening, and disrupting IT security thus endangers the basic functions of even the most unfree society in a modern, IT-supported world of ubiquitous IT systems. IT professionals have the ethical obligation to make it understood that there is no choice in any kind of society but to not let cyber warriors determine the degree of safety and security of an information society.

Now that we have glimpsed the scope of cyber warfare activities employed, it is of utmost urgency to develop a common understanding of citizens, private enterprises and politics to sharply limit the scope of activities of clandestine agencies aimed at undermining the foundations of a civil information society.

References:

ACM Code of Ethics: http://www.acm.org/about/code-of-ethics

Aid, Matthew M.: Inside the NSA's Ultra-Secret China Hacking Group; in: Foreign Policy, 10. Juni, 2013; http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group?page=0,1

Ball, James; Borger, Julian and Greenwald, Glenn: Revealed: how US and UK spy agencies defeat internet privacy and security, Guardian Weekly, Friday 6 September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[49] James Ball, Julian Borger and Glenn Greenwald: Revealed: how US and UK spy agencies defeat internet privacy and security, Guardian Weekly, Friday 6 September 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[50] Microsoft Security Research & Defense: Microsoft certification authority signing certificates added to the Untrusted Certificate Store, 3 Jun 2012, http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authoritysigning-certificates-added-to-the-untrusted-certificate-store.aspx

[51] On NSA and drone wars: Patrick Beuth: NSA hilft der CIA beim Töten, Die Zeit, 17th Oct. 2013, **http://www.zeit.de/digital/internet/2013-10/nsa-liefert-cia-daten-drohnen**. On Data from Germany for drone attacks: http://daserste.ndr.de/panorama/archiv/2013/panorama4781.pdf

BAMFORD,JAMES : THE PUZZLE PALACE. INSIDE THE NATIONAL SECURITY AGENCY - AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION. HARMONDSWORTH, 1982

Bamford, James : The NSA Is Building the Country's Biggest Spy Center (Watch What You Say); in: Wired. 15.03.2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/

Barry, John : The Nuclear Option: Thinking the Unthinkable; in: Newsweek, 14.01.91, S. 12-13.

Beuth, Patrick : NSA hilft der CIA beim Töten, Die Zeit, 17th Oct. 2013, http://www.zeit.de/digital/internet/2013-10/nsa-liefert-cia-daten-drohnenHYPERLINK "http://www.zeit.de/digital/internet/2013-10/nsa-liefert-cia-daten-drohnen"

Bundesministerium des Inneren: Cyber-Sicherheitsstrategie für Deutschland, Berlin, Feb. 2011, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

Campbell, Duncan : How NSA access was built into Windows; Telepolis, 4.09.1999, http://www.heise.de/tp/artikel/5/5263/1.html

Florencio, Dinei; Herley, Cormac: Sex, Lies and Cyber-crime Surveys, Redmont, June 2011, http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf

Gellman,Barton; Nakashima, Ellen: U.S. Spy agencies mounted 231 offensive cyber operations in 2011, documents show; in: Washington Post, 31. Aug. 2013; http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration

Gorman, Siobhan: Costly NSA initiative has a shaky takeoff, Baltimore Sun, Feb. 11, 2007, http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa

Gostev, Alexaner : Kaspersky Security Bulletin 2012. Cyber Weapons, http://www.securelist.com/en/analysis/204792257/Kaspersky_Security_Bulletin_2012_Cyber_Weapons.

Kaspersky Lab: Research Proves that Stuxnet and Flame Developers are Connected, June 11, 2012, http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected

Kushner, David: The Real Story of Stuxnet; IEEE Spectrum, 26 Feb 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Liles, Samuel: Cyber Warfare: As a Form of Low-Intensity Conflict and Insurgency; Conference on Cyber Conflict, NATO CCD COE Publications, 2010

Lischka, Konrad; Stöcker, Christian: NSA-System XKeyscore: Die Infrastruktur der totalen Überwachung; Spiegel Online, 31.07.2013; http://www.spiegel.de/netzwelt/netzpolitik/xkeyscore-wie-die-nsa-ueberwachung-funktioniert-a-914187.html;

McAfee: Virtual Criminology Report 2009. Virtually Here: The Age of Cyber Warfare, Santa Clara, 2009, http://resources.mcafee.com/content/NACriminologyReport2009NF

Nakashima, Ellen; Miller, Greg; Tate, Julie: U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say; in: The Washington Post, 19.06.2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html

National Security Council: The Comprehensive National Cybersecurity Initiative (unclassified), Washington, March 2010, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Peterzell, Jay: Spying and Sabotage by Computer. Time, March 20, 1989, S. 41

The President's Commission for Critical Infrastructures Protection, Washington, 1997, http://www.iwar.org.uk/cip/resources/pccip/backgrd.html

Sanger, David E.: Obama Order Sped Up Wave of Cyberattacks Against Iran; New York Times, June 1, 2012, p. A1; http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Schmidt, Jürgen: Todesurteil für Verschlüsselung in den USA; Heise Security, 4.10.2013, http://www.heise.de/security/artikel/Todesurteil-fuer-Verschluesselung-in-den-USA-1972561.html

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

Simonite, Tom: Digitale Geister, die ich rief; in: Technology Review, 02.03.2012, http://www.heise.de/tr/artikel/Digitale-Geister-die-ich-rief-1446457.html

U.S. Army Field Manual 3-13 "Information Operations: Doctrine, Tactics, Techniques, and Procedures", Washington, November 2003, http://www.iwar.org.uk/iwar/resources/doctrine/fm-3-13.pdf .

U.S. Department of Defense: Field Manual 1-02, Operational Terms and Graphics, Sept. 2013, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adrp1_02.pdf

U.S. Department of Defense: Field Manual 3-36, Electronic Warfare, Nov. 2012, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/FM3_36.pdf