IRIE
International Review of Information Ethics ISSN 1614-1687

Vol. 20 (12/2013)

Cyber Warfare

edited by Jürgen Altmann, Francesca Vidal

Editor of this issue:

Jürgen Altmann

Dept. Experimental Physics III
Technical University Dortmund, Germany
Email: altmann@e3.physik.uni-dortmund.de

Francesca Vidal

Dept. Philosophy
University Koblenz-Landau, Landau, Germany
Email: vidal@uni-koblenz-landau.de

Editors of IRIE

Vol. 20 (12/2013)

Content:

  ISSN 1614-1687

Editorial: On IRIE Vol. 20

Cyber warfare - when we planned this issue already some time ago we thought of being once again on the leading edge of reflecting the implications of ICTs on global society and our modern life. And once again we have been surpassed by reality.

At first, if we look at the various physical war zones of today we can see more and more cyber weapons in place and in heavy use as well. Nearly every warring party blames the other of using means of hacking to conduct sabotage or espionage in the course of the physical acts of war. And yes, you can bomb the power plant of your opponent or 'stuxnet' it – and of course as the missile can be misguided the virus could also infect the IT infrastructure of a hospital instead. No, a cyber war is not a clean war by definition. But then, what is the difference of killing a combatant with a gun or by a click?

Yet, much more attention has been drawn to the debate of cyber warfare where there is no physical war taking place at all. China and the US e.g. are not at war with each other (at least in the classical sense of having diplomatically declared it to be so or having crossed each other's borders with armed forces wearing uniforms). But in the cyber sphere they do cross their virtual borders all the time and they do attack each other. Let us not be naïve: it is not that they just suspect or blame each other to do so (what they extensively do) – as a matter of fact they are if not yet at war at least testing their capabilities and continuously increase them. Even if the scale is yet more comparable to shooting bullets across the border than to deploying heavy artillery but yes, we have entered this new dimension of the digital sphere now also in the area of warfare. And according to the rising budgets spent every year to improve the effectiveness as well as the camouflage of the respective techniques one can easily foresee their growing importance and also assume their probable social dominance one day.

And that leads to what finally makes the debate red-hot at the very moment: the threats of cyber war or even cyber armament for the civil society also in times and zones of alleged peace. In the name of defending against terrorism and counter espionage and being prepared for possible physical and cyber attacks the super powers have launched an unprecedented ICT infrastructure of mass surveillance and control and do not hesitate to use it also against friendly nations as the NSA scandal made publically clear. Our privacy is under attack by military forces at the very moment. And one could ask if this happens for a greater good. But that only confirms that it happens.

So if cyber war has become a reality even if on a very small scale that one wouldn't call a war yet and if the means of cyber warfare do not stop at concerning also the civil society what is more demanding than asking for ethical reflection of these developments. For the very interesting yet not calming answers please see for yourself in this issue - small in size but rich in content.

Yours,

the editors.

ISSN 1614-1687

Jürgen Altmann, Francesca Vidal:

Ethics of cyber warfare

The Internet has opened up tremendous new possibilities for the exchange of information. It has become one pillar of modern life. It is a global network that has to be available continuously for the functioning of economy and policy as well as private households. At the same time it constitutes a fragile infrastructure that can be disturbed – or used for malicious purposes. The principal possibilities range from manipulation or deletion of data to interference with critical infrastructures. Criminals attack servers and plant worms or viruses on computers to draw money from others' accounts or to spy on secret information. Hackers invade networks for protesting.

Even though such actions often require deep knowledge and considerable sophistication, they are dwarfed by far by state preparations for cyberwar. The US has declared cyberspace the fifth domain of military operations, beside land, sea, air and outer space. Other countries follow this precedent.

Whereas protection and defence against cyber attack is clearly legitimate, preparations for cyber offence raise many problems and can become very dangerous. Attacks in cyberspace can have direct consequences in the real world. Indirectly they can lead to counter-attack by real weapons. Cyberwar and its links to real-world war present challenges for security policy and international law, as can be seen in a developing body of academic and practical literature and differing approaches, still in flux, by various countries.

New possibilities of warfare also pose questions with respect to ethics. Here the issues are not only ethical assessment of virtual attacks and the consequences in reality, but also consequences that military preparations for cyber warfare can have on the civilian use of the Internet. Other aspects are: How could the infrastructure of ubiquitous communication be used malevolently? How do different countries deal with the problem of (national and international) security in cyberspace?

To shed light on such questions to do with the ethics of cyber warfare, the present issue of the International Review of Information Ethics presents four articles.

In his paper "*Cyber War: Will it define the Limits to IT Security?*" Ingo Ruhmann shows that cyber warfare is one part of military information operations that have a long tradition. Existing gaps in civilian information security and insufficient law enforcement, in particular due to the international character of the Internet, are being used as arguments for offensive military preparations. They are directed against a very broad range of potential adversaries, including civilians and allies. IT security is increasingly moved from the civilian to the military domain. Surveillance, espionage and IT system manipulations – alleviated by forced co-operation by the IT industry –violate legal and ethical principles and undermine the foundations of a civil information society.

Also Ute Bernhardt's essay "*Google Glass: On the implications of an advanced military command and control system for civil society*" deals with the modification of civil society through wide-spread information and communication technology and the ethical implications. She describes the possibilities of using augmented reality at the example of Google Glass. Military uses of head-mounted displays and networking of soldiers have a twenty-year history. Civilian uses, in particular in co-ordinated groups with central supervision, open new possibilities for observation by police or intelligence, for crimes and their rehearsals, and for terrorist attacks. Since incorporating countermeasures against criminal uses would be difficult and convincing arguments for legitimate uses in the civilian sphere have not been made, Google Glass-like systems pose the question whether IT professionals can ethically approve the work on such systems at all.

In his paper "*Uma análise sobre a política de informação para a defesa militar do Brasil: algumas implicações éticas*" (*An analysis about the information policy for the military defence of Brazil: some ethical implications*) Bruno Nathansohn analyzes the development of the Brazilian defence information policy particularly in regions of Brazil's geostrategic importance. The Brazilian government faces a dilemma between international cooperation based on a multilateral perspective on the one hand, and the threats to its information infrastructure arising from this cooperation on the other. The fragility of the Brazilian information infrastructure is due to the

ISSN 1614-1687

lack of an appropriate information policy that could and should support the role of the country in the international power system. The paper deals with these issues as related particularly to cyber warfare from an ethical and legal perspective.

The article "*Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia*" written by David Gorr and Wolf Schünemann deals with the emerging policy field of Internet governance in general and the challenge of cybersecurity in particular from a political science perspective. After some theoretical reflections on the structural difficulties that the regulators of cyberspace 'naturally' face they present the social-constructivist concept of securitization in order to explain how the internet is frequently constructed as a security problem by societal actors in different countries as well as on the international level. Finally, they illustrate their observations by a comparative analysis of cybersecurity discourses and dispositives in Germany and Russia.

All in all these articles add important considerations to the on-going debate on the ethics of cyber warfare. We want to thank the authors, but also the anonymous reviewers who contributed much to the preparation of this special issue.

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

Ute Bernhardt:

Google Glass: On the implications of an advanced military command and control system for civil society.

Abstract:

In the early 1990ies, the U.S. Army presented the first experimental units of a future soldier's equipment, featuring a soldier with a networked video camera, various sensors, and connecting the system to the world wide military command and control network. In June, 2012, Google unveiled its prototype Google Glass, a device capable of video and audio capturing with additional augmented reality functions.

In this article, a comparison between those military and civilian augmented reality systems and typical application settings will be used to ask for the implications of this kind of technology for the civil society. It will especially be focused on the consequences for civil safety, when the full range of cooperation capabilities available with Google Glass-like devices will be employed by organized groups of criminals or terrorists. In conclusion, it will be argued to assess the implications of this technology and prepare for a new degree of coordination in the activities of groups in the civilian space.

Agenda:

Author:

Ute Bernhardt

- c/o FIfF e.V., Goetheplatz 4, 28203 Bremen
- eMail: ute@kriton.bn.shuttle.de, http://fiff.de/themen/ruin/ruestung-und-informatik/materialien-und-dokumente/
- Relevant Publications:
  - Ute Bernhardt: Video: die unkontrollierte Überwachungstechnologie; in: Datenschutz-Nachrichten, 11. Jhg., Heft 1, 1988, S. 4-10
  - Ute Bernhardt; Ingo Ruhmann (Hrsg.): Ein sauberer Tod. Informatik und Krieg. Marburg, 1991
  - Ute Bernhardt: Maschinen-Soldaten. Der Mensch auf dem modernen Schlachtfeld; in: dieselben: Ein sauberer Tod. Informatik und Krieg, Marburg, 1991, S. 154-162

ISSN 1614-1687

- Ute Bernhardt, Helga Genrich, Ingo Ruhmann: Der Prozeß Verantwortung; in: Hans-Jörg Kreowski (Hrsg.): Informatik zwischen Wissenschaft und Gesellschaft. In Erinnerung an Reinhold Franck, Informatik-Fachberichte, Band 309, Berlin, 1992, S. 242-254
- Ingo Ruhmann; Ute Bernhardt; Dagmar Boedicker; Franz Werner Hülsmann; Thilo Weichert: An Appraisal of Technological Instruments for Political Control and to Improve Participation in the Information Society. Study for the Scientific and Technological Options Assessment Programme of the European Parliament. Directorate General for Research, Luxembourg, January 1996, PE: 165.715.
- Ute Bernhardt; Ingo Ruhmann: Von der Verantwortung der Informatiker; in: Werden 97/98. Jahrbuch für die deutschen Gewerkschaften. Frankfurt, 1997, S. 185-193
- Ute Bernhardt: Das Imperium schlägt zurück. in: Gerfried Stocker; Christine Schöpf (Hrsg.): Information.Macht.Krieg. Tagungsband der Ars Electronica 1998. Wien, 1998, S. 154-162
- Ute Bernhardt, Ingo Ruhmann: On Facts and Fiction of „Information Warfare". in: Bernhelm Booß-Bavnbek; Jens Høyrup (Eds.): Mathematics and War; Basel, 2003, S. 257-281
- Jürgen Altmann, Ute Bernhardt; Kathryn Nixdorf, Ingo Ruhmann, Dieter Wöhrle: Naturwissenschaft – Rüstung - Frieden. Basiswissen für die Friedensforschung. Lehrbuch. Wiesbaden, 2007
- Ingo Ruhmann, Ute Bernhardt: Information Warfare und Informationsgesellschaft. Zivile und sicherheitspolitische Kosten des Informationskriegs. In: Wissenschaft und Frieden, Heft 1/2014, Dossier Nr. 74 http://wissenschaft-und-frieden.de/seite.php?dossierID=078

A Google Glass system, looking quite like a small pair of stylish glasses, is an Augmented Reality (AR) system with a head-mounted display (HMD). Data related to the situational context are automatically displayed into the wearer's field of view. Pictures, audio or video feeds taken by the built-in microphone and camera are transmitted to other users or onto a cloud server where they can be stored or used to recognize people potentially by face recognition – which is until now not offered by Google, but available as a third-party app[1] - or by other personal attributes. Google Glass aims for ease of use through hands-off-controls with voice commands. It thus is a powerful AR gadget with autonomous computing power and connectivity[2]. The system has the perspective to add other sensors the user might find useful. Google Glass is only the most prominent of various systems with common properties on the market[3], and even more are under development[4]. The conclusions in this article are not restricted to a certain product, but are valid for any HMD AR device with comparable properties.

The intense publicity and the data made available on Google Glass have caused a debate on the system's potential as a tool for surveillance and the imbalance of knowledge between ordinary persons as bystanders on the one side and Google Glass users on the other side. The system's capability of instant video analysis with the power of recognition and identification – based on the rather imperceptible use of mobile connectivity with the computing power of Google's servers - is advertised as giving the Google Glass wearer utmost information about his or her surroundings including data on individuals in the field of view. Regardless whether the system works or will be marketed as advertised, Google Glass promises its users to end anonymous encounters with others in the real world. Google Glass is all the better in urban areas with good connectivity and enough tech-savvy people to look inconspicuous.

The debate on ethical issues to date has mostly concentrated on privacy issues, loss of control, reputation and autonomy[5] of those watched by a Google Glass user, what it means to be subjected to individualized video surveillance in interactions with these users and the possible follow-on analysis of the footage on Google's servers[6].

But these discussions center around Google Glass-like HMD systems only connected to web resources and used by individuals. Although Google promotes Glass with collaboration and data sharing features[7] it has not at all

---

[1] The MedRec app offered in 2013 can look up patient records by taking a picture of their face; http://glass-apps.org/medref-google-glass-app. At the CCC Congress in December 2013, Lambda Labs announced a face recognition app not supported by Google: Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Online, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

[2] See the descriptions and reports at: http://www.google.com/glass/start/

[3] Most mentionable of the others are the readily available products Recon Jet HMD (http://reconinstruments.com/products/jet/) , Epiphany Eyewear (http://www.epiphanyeyewear.com/), GlassUp from Italy (http://www.glassup.net/) and the Vuzix Smart Glasses accessory to smartphones (http://www.vuzix.com/consumer/products_m100.html). Even the Nissan car company presented an AR device called "3E" in November 2013: The 3E View of the Tokyo Motor Show, Nov. 19, 2013, http://blog.nissan-global.com/EN/?p=11271

[4] Google Glass-Like Products Can Launch For As Low As $400, Forbes, 21.07.2013; http://www.forbes.com/sites/haydnshaughnessy/2013/07/21/google-glass-like-products-can-launch-as-low-as-400/. Microsoft is reported to test an AR prototype, developed since some time: Microsoft Tests Eyewear Similar to Rival Google Glass, Wall Street Journal Online, 22nd Oct. 2013, http://online.wsj.com/news/articles/SB10001424052702304402104579150952302814782. Samsung has filed patents for its developments: Samsung files patent for Google Glass-like device, San Jose Mercury News, 25.10.2013, http://www.mercurynews.com/business/ci_24386791/samsung-files-patent-google-glass-like-device

[5] See for example European Network and Information Security Agency (ENISA): To log or not to log? - Risks and benefits of emerging life-logging applications, 2011; http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/life-logging-risk-assessment; Katina Michael and M.G. Michael: Computing Ethics: No Limits to Watching? Communications of the ACM, Nov. 2013, p. 26-28

[6] See Mark Hurst: The Google Glass feature no one is talking about; Feb. 28th 2013, http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about/

[7] See "Even share what you see. Live"; http://www.google.com/glass/start/what-it-does/ and the Throughglass App: http://glass-apps.org/throughglass-google-glass-app

been reflected, to what effect Google Glass might be used by groups of users. What happens in the transformation of Glass functions into a scenario of group support?

This is on the sender side the ability to capture the scene at hand and transmit it to others, and on the receiver end the ability to access data on the same scene and relevant data elements in it, and for all collaborators, to act in a coordinated manner. In an individual mode, both of these functions may seem nice, but lack a convincing functional model. Such a coherent model emerges, when a Google Glass user is seen as a node in a collaborative network producing input for him- or herself as well as others and receiving support out of the data and the activities of others. The automated reality augmentation in applications available today on smart phones – irrespective of their different kind of display style – is often little more than data on the vicinity of a certain location found on Google Maps. It is by far more convincing when a kind of external supervision or other ways to exchange AR items between users comes into play that vastly enhances the potential of Google Glass for its users and has additional consequences for a bystander or the addressee of a Google Glass-empowered group[8].

A glimpse of what is to come in Google Glass groupware can until now only be seen as mockups: Google Glass Games for individuals and groups[9], amongst them a Google Glass ego-shooter[10]. This mock-up ego-shooter and other ideas by Microsoft represent a return to the origins of the development of HMD-based AR systems.

Origins of head-mounted augmented reality systems

In 1993 the U.S. Army conducted several maneuvers to experiment and assess newly developed experimental equipment for ground soldiers in combat. In the so-called Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration, a group of soldiers only one-third the size of ordinary units ambushed a much larger force, occupied and secured various positions in an open field as well as in a city setting.

The group used sensory augmentation from digitally enhanced video cameras, laser and infrared sensors as well as augmented long-range hearing. Through the exchange of data and through navigation and range-finding equipment the soldiers were able to locate and triangulate their adversaries' positions by passive means without notice and mark them on a common battlefield map displayed in their HMD's AR display together with other data sources. In difficult terrain and in close urban combat, they could use a video camera to look around obstacles, avoiding danger and being noticed. The soldiers exchanged video and audio footage taken of the battlefield independent of weather conditions to achieve a common picture on their adversaries' actions before starting their attack. All data from the battlefield were continually transmitted to a command post, where further intelligence was collected and transmitted back to the soldiers.

Full connectivity between soldiers and between them and a command and control network provide the means to exchange all relevant data as needed. AR in a HMD worked as a hands-off technology and augmentation of perception with complex data on the battle area and the friendly and enemy action developing on it. All combined proved to be a vastly more effective way of combat, so that such systems are rated as "force multipliers". A significantly smaller number of soldiers - by better coordination and access to external sensor data – could achieve a higher lethality at greater distances with fewer losses in a highly intensified battle:

> *The soldiers were able to "accurately direct a lethal volume of fire onto objectives beyond current night vision device ranges and provide the ability to use more smoke and still place effective fire on the objective.*

[8] This of course is also valid for other products of this kind: Microsoft is reported to patent AR glasses for multiplayer games, see: Microsoft tries to patent AR glasses for multiplayer gaming, engadget, 2.08.2013, http://www.engadget.com/2013/08/02/microsoft-ar-glasses-for-multiplayer-gaming-patent/

[9] Simon Parkin: ButtonMasher: First AR games for Google Glass emerge; New Scientist, Nov. 1st, 2013; http://www.newscientist.com/article/dn24505-buttonmasher-first-ar-games-for-google-glass-emerge.html

[10] http://www.youtube.com/watch?v=QxG5xNktqw0

> *With improved communications, response time for fire control is reduced. […] It will also aid in the detection of the enemy's presence before the soldiers themselves are detected." [11]*

These results with experimental technology - that can be traced back to demonstrators from the mid 1980s[12] - have since been translated into the requirements for the ground force of the 21st century. The so-called Force XXI concept was developed in the U.S. to allow for a military engagement of small groups and making full use of information technology to intensify and improve fighting capabilities:[13]

> *"The concept for Force XXI Operations is centered around quality soldiers and leaders whose full potential is more closely realized through information age technologies and by rigorous and relevant training. […] It describes an operational environment where the acquisition, processing, and rapid sharing of information revolutionizes the conduct and tempo of operations." [14]*

The integration of the individual ground soldier into the command and control network and its equipment with real-time data gathering and sharing technology, as well as augmented reality-capable displays is progressing at full speed: Currently, the U.S. Army integrates the "Force XXI Battle Command Brigade and Below" as the digital command and control system for "automatically disseminating throughout the network timely friendly force locations, reported enemy locations, and graphics to visualize the commander's intent and scheme of maneuver" [15]. The next stage will be deployed as a mobile battlefield network for sharing of data and "information via voice, data, and real-time video"[16]. The pictures of U.S. President Obama following live the raid on Osama bin Laden's hideout in Pakistan in a command room showed the world the use of fully connected ground forces in combat.

Although most of these HMD-based military AR applications still do not seem to be perfect in their performance, robustness and accuracy needed in combat, the tactical advantages of the systems developed are obvious enough to see quite a number of different HMD models for AR applications in substantial quantities in various armies' combat missions[17]. Amongst other armies, the German Bundeswehr has proceeded from the concept stage in the program „Infanterist der Zukunft"[18] to battlefield use of the "Gladius" system with production line

---

[11] Victor Middleton, Ken Sutton, Bob McIntyre and John O'Keefe IV: Soldier Integrated Protective Ensemble (SIPE) Advanced Technology Demonstration (ATD), Dayton, Oct. 2000, p. 22f. . http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA384680

[12] See the description of the presentation by the British Company Scicon Computer Systems at the British Army Equipment Exhibition in 1984. This prototype of a soldiers's equipment was supposed to have full AR functionality with additional infrared vision in the integrated HMD display, see: Military Technology, No. 10, 1986, p. 166. Steven M Shaker, Robert Finkelstein: The Bionic Soldier; in: National Defense, April 1987, p. 27 – 32. Head-mounted displays for AR applications were first published as a scientific paper by T.P. Caudell, D.W. Mizell: Augmented reality: an application of heads-up display technology to manual manufacturing processes; in: Proceedings of the Twenty-Fifth Hawaii International Conference on System Sciences, 1992, Vol.2, pp. 659 - 669

[13] U.S. Army: TRADOC Pamphlet 525-5: Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, TRADOC Pamphlet 525-5, Fort Monroe, Aug. 1994, p. 2-1fff

[14] U.S. Army: TRADOC Pamphlet 525-5: Force XXI Operations, A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, TRADOC Pamphlet 525-5, Fort Monroe, Aug. 1994, preface

[15] U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems 2012, p. 108f

[16] In the "Warfighter Information Network-Tactical Increment 3" program, see: U.S. Department of Defense, Office of the Assistant Secretary of the Army: Weapons Systems Handbook 2013, p. 322f

[17] Michael M. Bayer, Clarence E. Rash, James H. Brindle: Introduction to Helmet Mounted Displays, p.47-107; in: Clarence E. Rash, Michael B. Russo, Tomasz R. Letowski, Elmar T. Schmeisser: Helmet-Mounted Displays: Sensation, Perception and Cognition Issues, Fort Rucker, Alabama, 2009; http://www.usaarl.army.mil/publications/HMD_Book09/

[18] Infanterist der Zukunft; http://www.deutschesheer.de/portal/a/heer/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK9jNTUIr2S1OSMvMxsvYLUouKC1Gy9zLy0xLySVP2CbEdFAPnFG_s!/

head-mounted displays (HMDs) for AR applications delivered to German troops in Afghanistan in 2013[19]. The revenues for AR systems on the battlefield are estimated to reach $8.2 billion by 2016[20]. Advanced systems are under development that no longer need any glasses at all, but project data onto contact lenses[21].

Internet of Warriors

Equipping soldiers with AR-capable HMDs and networking them does not only aim to maximize the single warrior's effect, but tries to extend the reach of command to the last independent actor on the battlefield. Officers get immediate control over actions by any individual soldier who automatically communicates his or her position, very often also live video feeds of their action and telemetric data. The Force XXI doctrine stated from the start that it would result in hierarchical organization forms existing in parallel to new network-centered forms in combat missions. These two seemingly conflicting structures come to a combined result, when AR technology on the battlefield is used by "quality soldiers": special forces. For the soldiers, it results in an improved "situational awareness", for their commanders in the data exchange loop, in a better "top sight" of the unfolding battle situation and taken together lead to markedly improved efficiency in small forces combat.

This result of improved command, control and communication capabilities through information sharing is nothing new in military development: The main battle tank appeared on the front lines in World War I, when it was used to breach fortifications and to shield infantrymen from enemy fire in an assault. In most armies, this was still the dominant tactic at the beginning of World War II. In contrast, the German army had equipped their tanks with VHF radio communications, and through command and communications formed a unified force of heretofore unknown speed and fighting power that changed the way ground wars are fought until the present day.

An analogous process is taking place on the battlefield. Soldiers are being equipped with sensors, cameras, computing power and communications equipment. The soldier becomes a node in the network of military command and control to interconnect the world of information warfare with actual fighting on the ground. The result will be the "Internet of Warriors": Just as the Internet of Things, where data are stored in production items and used to control the production line, soldiers in the "Internet of Warriors" are supposed to act autonomously and collaboratively against their adversaries and feeding data back to their commanders.

Information Dominance

"Top sight" and "situational awareness" for ground forces are synonyms of a warfighting doctrine of modern armies that centers around a better knowledge of the situation on the battlefield. The improved knowledge of a tactical situation is used to assess the plans of an adversary, and to act preemptively with the aim not only to outmaneuver opposite forces, but to influence their assessment of the situation, thus ultimately modifying an enemy's perception of battle. This can obviously be achieved through conventional camouflage. In the age of distance sensors, however, this camouflage and work on situational perception has moved to the digital realm and means the disruption and alteration of any sensor data, of data communication and of data processing in any kind of IT equipment – regardless if in military or civilian systems. The term used for this IT-

[19] Drittes Auge für Deutsche Soldaten; Spiegel Online, 20.02.2013; http://www.spiegel.de/wissenschaft/technik/militaertechnologie-bundeswehr-will-gladius-system-einfuehren-a-884238.html; see also the Rheinmetall press release: http://www.rheinmetall.com/de/rheinmetall_ag/press/news/archive2012/news_details_5_1664.php

[20] Mind Commerce: Augmented Reality in the Battlefield 2012 – 2016, July 2012, ASD Report, Amsterdam 2012; https://www.asdreports.com/shopexd.asp?id=32490

[21] Babak A. Parviz: Augmented Reality in a Contact Lens. IEEE Spectrum, 1st Sept. 2009, http://spectrum.ieee.org/biomedical/bionics/augmented-reality-in-a-contact-lens

related disruption of perception, in the terminology of the most advanced army in this discipline, is "Information Dominance".

After years of conceptual development and actual application in warfighting, the U.S. Army has refined its operational repertoire from a rather broad approach of Information Warfare to a quite detailed definition of so-called „Inform and Influence Activities"[22]. In short, Inform and Influence Activities start with public relations, cover electromagnetic and cyber activities, encompass all data sharing in the Theater of War and end with physical attack on the battlefield. This broad view is by no means new, but has been used since the end of the 1990s[23] and especially encompasses the capabilities of soldiers equipped to Force XXI standards.

Contrary to common perception, the term "Cyber Warfare" is not in the official vocabulary of the U.S. Forces. "Cyber Warfare" can only be found as a tool in Electronic Warfare[24]. In the literature, cyber warfare is used as a synonym for a disruptive use of manipulation tools in computer networks and described as a tool in low-intensity, often asymmetrical conflicts[25]. The equivalent official DoD term is "Information Operations" encompassing all "information and information systems and to influence decision making"[26].

It is obvious that the development of ground combat to a stage that rests on fully IT-equipped soldiers and the interconnection to a command and control network, necessarily implies undisrupted IT and communications systems: "Information Assurance is the cornerstone of the strategy for ensuring information dominance in a net-centric warfare environment" [27].

It has become impossible to decouple physical and digital operations. Applying cyber and electronic warfare operations in counterinsurgency means - amongst other tasks - to prevent the detonation of explosive devices and facilitate the disruption of many other command and weapons systems of insurgents. In an age when improvised explosive devices are remotely controlled by mobile phones, applying a smart phone computer trojan in a battlefield setting obviously has a physical and possibly lethal effect. The interdependency of digital and physical world has also been demonstrated by the Stuxnet computer trojan: It was physically mounted at the uranium enrichment site by USB stick and physically damaged machinery at this and other locations.

The Internet of Warriors blurs the distinction between digital and physical battle. Cyber Warfare Operations thus must strictly be seen as the small section of Information Operations that have a very broad range and employ very different means.

Enter Google Glass

Comparing the technical features, Google Glass and comparable products – that are used synonymously here - are a somewhat reduced version of typical HMD systems found in military use today. The Android operating system version for Google Glass makes app development easy. Irrespective of further modifications in the software of the system, it can safely be assumed, that a civilian HMD device equipped like Google Glass will be available in the near future that either is useful for special demands or can and will be modified to any dedicated

[22] U.S. Department of Defense: Field Manual 3-13, Inform and Influence Activities, Jan. 2013, p. 1-1

[23] See: Ute Bernhardt, Ingo Ruhmann: Informatik; in: Jürgen Altmann et al.: Naturwissenschaft – Rüstung – Frieden; Wiesbaden, 2007, p. 392ff

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

[25] 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

[26] U.S. Department of Defense: Field Manual 1-02, Operational Terms and Graphics, 2004, p. 1-99

[27] Association of the United States Army: Information Assurance - Defending and Securing Army Networks and Systems. August 2006. p. 11, http://www.ausa.org/publications/torchbearercampaign/tnsr/Documents/TBSecRepAug06.pdf

users' special demands – be it only for gaming purposes, incentives for efficient modifications are clear enough to see.

Because Google Glass captures and displays data strictly in relation to the location or the people in the vicinity of its user, a group collaboration with Google Glass can be safely assumed to mostly use the same categories of data relating to the current location or the social interaction of Google Glass users. A foreseeable and simple civilian application, that only slightly extends today's smart phone apps, will be the interactive Google Glass wayfinding, where a Google Glass user is steered by another person – looking at the video image taken by the Glass device - through a location by augmenting direction cues into the HMD and highlighting points of interest.

Now let us replace "points of interest" with "persons" being highlighted and tagged in the HMD by some remote party. This not only makes identification easier but – through four or more eyes looking at the same detail of reality captured on live video – clearly eases the pursuit of target subjects even in the most crowded locations. Couple this with the range finding and passive position triangulation of third parties by two or more Google Glass users seen already in the SIPE maneuvers in the 1990s. Today's technology is additionally able to automatically track the features of the target subject and share the data amongst all Google Glass participants once the tagging has been done. So, with only these minimal additional properties easily realized by software, one can have an exciting time together in an AR-enhanced reality adventure game - or do the duties of police or secret service officers, or groups of criminals or terrorists following their victim. That the Google Glass communication gear, made for imperceptible use, eases the coordination and reduces the danger of one's cover being blown, is an additional support for clandestine observation groups.

Now let us go one step further adding more sophisticated elements. Since HMDs have been shown to – in principle - integrate all sensors made available for data exchange on the scene, one can replace the video images with infrared and night vision equipment for operations in darkness or of hunting warm body signatures in hiding places in rugged or urban terrain. This, too, is an attractive gimmick for today's outdoor gaming scene. It is also very useful for policing and many illicit activities directed against third parties.

One can just as well add civilized versions of electronic warfare equipment for direction finding and identifying cell phones, or WLAN emitters – just a slight modification of the equipment on your smart phone - and other frequencies, and tagging the emitter locations together with their identifiers in the HMD's field of view. You thus can pinpoint mobile phone users in the field of view of your Google Glasses, helpful for hot pursuit in a criminal investigation.

Or one can just as well find and mark hidden sensors and intrusion alarm equipment relaying data by radio like a perimeter surveillance camera. More sophisticated tools might even identify such sensors by their relay patterns, instantly looked up on the web, and automatically or by remote advice suggest ways to circumvent them. Remotely controlling non-experts with the proper instrument and advice on burglar alarms can prove to be a vastly more intelligent way to have crimes committed than showing up on a crime scene oneself.

And if necessary, one can drive the practice of mobile phones modified into exploding devices one step further. One just has to convince someone to carry around some kind of sealed container, and transmit back Google Glass live video footage with the result, that the explosive device in the container can be triggered at the most effective moment.

All of these Google Glass scenarios are just very slightly beyond the actual technology available, which mostly means less than one year of development time. But even here, technology is of no use without experienced users and a reason for the application of novel technological means. Let me therefore describe just three scenarios to shown the advantages and likelihood of the use of Google Glass-like systems.

1. Legal observation by police or intelligence often is a difficult and resource-consuming business. The use of radio trackers or silent SMS's on mobile phones for location determination shows the effort to use more sophisticated technology to be less dependent of purely optical means. Google Glass as a group collaboration tool can be used to alleviate observation. As a prerequisite, any group of Google Glass users can bring a variable and mobile set of sensors anywhere these are needed, and have them – by GPS – pinpointed on the map allowing for passive position triangulation. Through common sensor

fusion algorithms or by manual assistance in a coordination center, all sensorial input about the target person can be fused to accurately and reliably follow and keep track of a target independent of any weather condition.

Since observation no longer would have to rest on a limited number of persons shadowing a target person, observation techniques might be changed altogether from a system of man-marking into a system of zone defense: A number of Google Glass users might follow one or more target persons, marked by tags in their AR visions, and hand over targets when they leave the observation zone. The live video footage taken will produce evidence, if for example, an illicit transfer of goods shall be observed. The usefulness of this scenario starts with just an observation of pickpockets doing their work – or tech-savvy pickpockets looking for prey.

2. Meticulously planned heists are not confined to Hollywood films. Groups can plan, exercise and execute crimes, not just a bank robbery or an assault on an armored car. Of course, many terrorist attacks have also been exercised before execution. Any improvement to alleviate coordination by unobtrusive HMD devices while staging a succession of activities by a group of persons will undoubtedly be used to exercise and realize crimes that can consist of more steps and actors than today. Timing can be perfected, diversionary tactics tested. AR tools are being explicitly developed to open up the opportunity for even a complete dress rehearsal played through at the real location. Exercising with inconspicuous AR tools can give a well planned heist a new level of perfection.

3. Attacks by large terrorist groups on hotels and shopping malls have been staged in Mumbai, Nairobi[28] and of course many targets in Iraq and Afghanistan. With Google Glass-like HMDs such a group can operate on common knowledge about their exact positions, location data augmented into view, and visual and auditory information on the activities by all group members just like in military maneuvers. At the beginning of the attack, the group can move decisively and simultaneously at different points against security guards, before anyone can activate the alarm. As a second step, the group members can access specific targets in the location and cordon off an area as desired before any external help can arrive on the scene. Any critical access point can be kept under control cooperatively even from a distance; external sensors can be integrated into the network. As a third measure, the group can spread hostages to several different locations in the compound or building without losing control thus raising the stakes for evacuation raids by security forces. Finally and in case of a raid, fully networked group members nullify the moment of surprise, since even a dead terrorist may still transmit the video and audio stream of the surroundings, alerting every other one in the loop.

Google Glass-like HMDs in civilian contexts provide the equipment and force augmentation for attacks that until now strictly required highly trained professionals. One may not forget, that conventionally equipped professionals - if possible - train a raid on a model of the situation at hand to reach a high level of cooperation. What they need as an exercise to gain the upper hand, a cooperation based on a Google Glass-like system would provide terrorists without that much effort.

Being watched by a Google Glass user might be an uncomfortable feeling, since one does not know, what data the Google Glass user might have accessed on the web and have in his or her display.

In a cooperative Google Glass scenario, a Google Glass user watching you might be in the same observation loop as someone totally unrelated some moments ago. One might even have entered a scene where a group of pickpockets scan for victims and coordinate their robberies by Google Glass. In a holdup or in a robbery, one might not know as a victim, whether an attacker is alone or supported by a Google Glass user nearby scanning the crime scene to cover the attacker. In an armed attack, the person with the gun and the Google Glass equipment is not the only pair of eyes and ears that might thwart an attempt to escape, but will rather be

28 As for example recently seen in a shopping center in Nairobi. Kenia (Drama in Einkaufszentrum: Präsident meldet Sieg über Geiselnehmer in Nairobi; see: http://www.spiegel.de/politik/ausland/praesident-meldet-sieg-ueber-geiselnehmer-in-nairobi-a-924322.html) Or see attacks in Pakistan and India: Hasnain Kazim: Angriff in Lahore: Taliban richten Blutbad in Moscheen an; Spiegel Online, 28.05.2010; ***http://www.spiegel.de/politik/ausland/angriff-in-lahore-taliban-richten-blutbad-in-moscheen-an-a-697393.htm***

connected to someone overlooking the scene and ordering to forcefully stop any escape or uncontrolled situation.

Enter security

Some future apps might prove to be highly useful in the scenarios described above. No one is expected to explicitly develop a "pickpocket support app" for Google Glass or something more elaborated for terrorist assaults. As a precaution against the legal problems already foreseen, a condition in Google's terms is that the company "may remotely disable or remove any such Glass service from user systems in its sole discretion" as Google "discovers a Glass service that violates Google developer terms or other legal agreements, laws, regulations or policies" [29].

How might violations be identified? Google Glass is the civilian version of a powerful command and control system. Google already reserved itself the right to store and use the user's location data, all the "photos and videos taken […] and [to] display information sent to devices that are synced with it"[30]. So Google is in the position to scan the data upon request or by itself to identify proper and improper use.

But there will also be demands by public authorities to exploit the data. Some technically inept petty criminals might get along with ordinary Google Glass features for their purposes. Even some terrorists sent on a suicide mission might be content with ordinary Google Glass features. Publicity for any such case will most certainly lead to the demand that Google Glass pictures and video feeds must be monitored in a manner comparable to today's CCTV systems. It will also be argued, that even innocent Google Glass users may visit areas of higher criminal activity ort security needs where they might accidentally and inadvertently take footage of illegal activities thus making it necessary to use Google Glass and other product's live feeds for general surveillance purposes.

The potential of Google Glass-like products for security purposes is enormous. The technology will give its users a huge boon for illegal activities as well as clandestine countermeasures by security forces.

As a way to prevent interference with illicit Google Glass uses and to circumvent surveillance, some of the scenarios described above will presume the skill and motivation of users to modify Google Glass and similar products to their specific needs. Since all Google Glass-like products have only restricted resources available, the options to tamper-proof them are limited. The Android operating system, Google Glass works on, is attacked by specific viruses, topping the mark of 100.000[31]. Google Glass was hacked only days after the first prototypes were given to developers giving full access to the system's capabilities[32]. One of the first Google Glass face recognition apps requires the hacking of the system to install it[33]. But the problem is not specific with the product: No embedded system with as limited resources as Google Glass-like products has yet withstood any dedicated digital engineering and attack. In consequence, one cannot assume any technological barrier against misuse in any of Google Glass-like systems to withhold modifications of the product beyond tight hardware

29 Google Glass Terms of Sale and use (as of December 2013); http://www.google.com/glass/terms/

30 Google Glass Terms of Sale and use (as of December 2013); http://www.google.com/glass/terms/

31 Kaspersky Security List: IT Threat Evolution: Q2 2013; https://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013#16

32 Entwicklerversion der Google Glass per QR-Code gehackt; http://www.heise.de/security/meldung/Entwicklerversion-der-Google-Glass-per-QR-Code-gehackt-1919373.html; based on: Lookout: Sicherheit für die vernetzte Welt: Ein Google Glass-Fallbeispiel; company blog, 17.07.2013, https://blog.lookout.com/de/2013/07/17/sicherheit-fur-die-vernetzte-welt-ein-google-glass-fallbeispiel/

33 Google Glass Face Recognition App Coming This Month, Whether Google Likes It Or Not; Forbes Onlie, 18th Dec. 2013, http://www.forbes.com/sites/andygreenberg/2013/12/18/google-glass-face-recognition-app-coming-this-month-whether-google-likes-it-or-not/

restrictions – for example the abdication of a camera or processors that self-destruct on tampering – that are costly or debilitating for the product.

Any of these developments are clearly disadvantageous for a bystander to a Google Glass user. For any innocent bystander, there will only be a slight difference in the level of discomfort between a legitimate Google Glass user confronting him or her, taking a live video feed that actually is or can be used later on for surveillance purposes extending today's stationary CCTV systems into a ubiquitous surveillance with anyone as a potential suspect as one option or an illicit user that has modified the HMD system to remain undisturbed while committing unlawful deeds as the other, making the bystander a potential victim.

Ethical Justification for Google Glass?

It is clear that applications will be developed for Google Glass-like products to be used in gaming or collaborative work whose features will allow the product's users to apply these features acting as a group against others. These features will be highly useful as a force multiplier for a wide range of unlawful activities. As Google Glass comes to the market, it can be expected that within the next five years "Google Glass Terrorists" will test this potential in their attacks.

Google Glass-like devices may have some advantages for crime enforcement and rescue operations by special military or police forces. However, these forces already have rugged HMD systems in their equipment. Military HMDs today are instruments for the Internet of Warriors and central to Information Warfare on the battlefield. Special Forces do not need any civilian version. They are the ones who would have to fight attackers vastly more dangerous through Google Glass-like devices. From a security forces perspective, Google Glass-like devices pose a clear danger.

The ethical questions posed by Google Glass and its likes are fundamental. First of all, it must be asked, if it is ethically sound to program apps that can easily be used for criminal activities. What feature combination of these systems could at maximum be tolerable to prevent a potentially highly dangerous technology to fall into the wrong hands? Is it realistic to assume such a reduced product to be competitive? Should there be a special code of conduct in developing these apps or bringing them on the market?

Could the effects of Google Glass and similar systems be alleviated by limiting the capabilities of these systems? If the system's set-up is left unchanged, reducing connectivity and bandwidth could be used as limiting factors making recording and transmission inconvenient. Automatically preventing the recording of sensitive situations or unwilling bystanders by the system through on-board image and sound processing is severely limited by the necessary computing power that will not fit into the design. Controlling Google Glass's use on the network end of the system would mean to employ a forced personal supervision on the transmitted data, since today's systems for automatic scene analysis assess the activities of the person in the field of view that, in the Google Glass case, will be not the Google Glass user, but a harassed bystander. Scene analysis or personal supervision of anyone in the field of view of a Google Glass system – that is, to collect data on a random set of bystanders and analyzing their behavior - to eventually prevent such a systems user's potential misbehavior is an extremely invasive and by no means reliable way to limit Google Glass misuse. Even if this would be legal – which it is not even in a majority of U.S. States – it would not result in the detection of aberrant behavior of the Google Glass user as the culprit and person responsible. So, surveillance of Google Glass use will more often than not lead to no detection of misbehavior whatsoever and thus would only help in the mass surveillance of bystanders.

Google Glass is an ideal instrument from another point of view. Modern warfare rests on the collection of data from all possible sources. The NSA and similar agencies collect communications data to track individuals and to spy on their plans. Surveillance drones are used to provide live coverage of their operation area. Google Glass users provide live coverage and recordings anywhere and on any human interaction imaginable – together with exact location data. Special forces are equipped with HMDs for exactly this reason. Google Glass provides a trove of valuable data for any military or secret service organization they simply cannot resist to use. The

broad communications surveillance by intelligence agencies that we can see today is a cornerstone of information warfare. The use of Google Glass and the data acquired will vastly extend this surveillance, opening up new dimensions for the application of information warfare tactics.

Google Glass is a technology that provides a high incentive for monitoring, which can have almost no effect for the user and originator but instead most certainly will have consequences for innocent third parties. Misuse may lead to a call for a better control of Google Glass users. But can there be an ethical justification for a mass surveillance of third parties as a way to potentially limit the misuse of Google Glass? Even if society would see the permanent surveillance by Google Glass users of any private interaction as a way to improved conformity and obedience to rules, this fundamental change in social interaction should be a result of debate - especially, because Google Glass as the instrument for obedience is not used by legitimate public officials against citizens, but between individuals. The second set of ethical questions therefore centers around the technology's control potential that is quite useless against the genuine perpetrators, but will mostly harm third parties and has disruptive potential for the society as a whole.

Since the basic design of these systems offers only limited security protection against tampering, ethical assessments should not be based on the idea that misuse might be prevented by the technical protection of specific app features or explicit design to leave some features incomplete or incompatible. The history of smart embedded systems with restricted resources shows, that with some effort there will always be a way to combine useful features to achieve unintended system properties useful for criminal acts. It has not yet been answered, that there are convincing legitimate uses for this technology in the civilian sphere. We must therefore finally ask a fundamental question: Can IT professionals ethically approve the work on such systems at all?

Conclusions

None of the producers of Google Glass-like systems has yet made any comment on the potential problems arising of this very special kind of collaboration features. No one in the IT world has yet spoken out to address the potential dangers of these systems to the general public. Google Glass, however, is only a symbol and the starting point for novel collaboration technologies for ubiquitous use. Now is the time to start a broad discussion on the implications for society, safety and security – before reality will teach us painful lessons.

The civil security authorities must assess the risks inherent in this technology and develop tactics to reduce the impact of a "Google Glass Terror Attack". Research is necessary to safeguard this kind of embedded and networked AR system against misuse. The companies involved must publicly be confronted with the responsibilities their product entails. And it is time to think, if work on these systems can ever be seen as an ethically responsible professional task.

Bruno M. Nathansohn:

Uma análise sobre a política de informação para a defesa militar do Brasil: algumas implicações éticas

Abstract:

An analysis about the information policy for the military defence of Brazil

Some ethical implications: It is presented the development of the information policy for the military defense of Brazil, taking into consideration information actions, which were implemented during the Brazilian history, and in the context of the regions where the country carries out geostrategic influence. The hypothesis is that there is a dilemma of the Brazilian state between cooperative international relations, based on a multilateral perspective, and the threats to its critical information infrastructure. Besides, technically there is a fragility of the cybernetics infrastructure because of the lack of an appropriate information policy, which could contribute to the position of Brazil in the international system of power, in accordance with its potentialities. Questions that imply ethics dilemmas about the threshold between the cooperative interchange, on the one hand, and the preservation of sovereignty, on the other, related with what should, or should not, be shared in the cyberspace.

Agenda:

Author(s):

MSc. Bruno Macedo Nathansohn:

- Pesquisador da Rede Latino-Americana de Geopolítica e Estratégia (RELAGE), Rua Xavier da Silveira, 22/Apto.601 – Copacabana – Rio de Janeiro/RJ CEP: 22061-010
- Tel.: +55 (21) 3204-1461; Cel.: +55 (21) 8228-7208; e-mail: bnathansohn@gmail.com; http://nathansohn.blogspot.com (Arquivo de Ideias)
- Relevant publications:
  - Estudo de usuários on line. Revista Digital de Biblioteconomia e Ciência da Informação. Unicamp. v.3, n.1 (2005). Bruno Macedo Nathansohn, Isa Maria Freire. p.39-59. Disponível em: http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/view/324
  - Um estudo sobre o processo de tomada de decisão política para a ação de inteligência: a possibilidade de gestão da informação arquivística. Perspectivas em Gestão & Conhecimento, João Pessoa, v. 3, n. 2, jul./dez. 2013. Bruno Nathansohn. p. 280-299. Disponível em: http://periodicos.ufpb.br/ojs2/index.php/pgc. ISSN: 2236-417X.

ISSN 1614-1687

Introdução

O governo brasileiro vem intensificando o desenvolvimento de ações para seu programa de defesa militar cibernética, o que está registrado na Estratégia Nacional de Defesa (END). Entretanto, o próprio Ministro da Defesa reconheceu, recentemente, que o Brasil não está preparado para se defender militarmente de um ataque à sua infraestrutura crítica de informação. Apesar da iminência de uma ciberguerra ser remota para o Brasil, existem indícios históricos de que atores estatais e não-estatais visem as riquezas proporcionadas pelo território brasileiro, o que inclui o monitoramento político do País. Vide as recentes operações de espionagem estadunidense contra o Brasil, os crimes de biopirataria na Amazônia por agentes de diversos países, a reativação da 4ª Frota estadunidense no Oceano Atlântico e as atividades do crime organizado nas fronteiras terrestre e marítima, o País busca desenvolver sua infraestrutura cibernética para o fortalecimento de seus laços políticos em fóruns como os do Mercosul e o da União Sul-Americana (Unasul). Torna-se primordial, nesse sentido, que haja primeiramente a construção de marcos institucionais que orientem a produção e os usos das Tecnologias de Informação e da Comunicação (TIC) para a defesa dos países considerados periféricos no sistema internacional. Essa perspectiva tornar-se-ia viável se a estratégia de defesa fosse orientada por princípios cooperativos, regidos por uma eficiente política de informação.

"A TI é usada para gerenciar as forças militares – por exemplo, para o comando e o controle e para a logística. Além disso, as munições guiadas com precisão ilustram como o uso de TI, integrada aos sistemas de armas, aumenta sua letalidade e reduz o dano colateral associado com o uso de tais armas. Movimentos e ações de forças militares podem ser coordenados através de redes que permitem obter informação e imagens por quadro do campo de batalha para serem amplamente compartilhados"[1]. (**Tradução nossa**: LIN, 2012)

Nos últimos tempos, o Brasil vem se notabilizando pela busca de relações internacionais multilaterais que valorizem acordos político-institucionais, e não restritos à competitividade mercadológica. A valorização dessa perspectiva pode indicar uma tendência contra-hegemônica nas relações internacionais pela centralidade das relações Sul-Sul, em detrimento de relações marcadas pela desigual Norte-Sul. A política externa brasileira orienta-se, em certa medida, por trocas mais equânimes entre atores que compartilham experiências históricas e condições sociais, políticas e econômicas semelhantes. Nesse sentido, ao contemplar relações simétricas, sob a lógica cooperativa, tende-se a relativizar a compreensão dos usos da técnica em relação à política. Isso não significa que o Brasil e os Estados que questionam o sistema hegemônico não se utilizem da técnica para alcançar seus objetivos de poder, muito pelo contrário. Entretanto, ao apresentar canais para a cooperação, tende-se a diluir o discurso e as práticas assimétricas entre os atores políticos, propiciando outras possibilidades de relacionamento para a diminuição das desigualdades interestatais e a resolução de conflitos.

Isso não que dizer também que a cooperação só seja possível e realizável entre atores que apresentem posições simétricas no cenário internacional, muito pelo contrário. A cooperação também pode ocorrer entre atores estatais e não-estatais, situados em condições absolutamente díspares. Todavia, o que consolidará relações mais ou menos sólidas entre os atores será a natureza das necessidades que compartilham e o nível de estabilidade política entre eles. Assim, o desenvolvimento de uma política de informação para a concretização de ações de informação dependerá da capacidade tecnológica dos atores em desenvolver e utilizar recursos de informação. O posicionamento do Estado, e da lógica de sua política de informação, no contexto internacional, será definido por meio dos usos dos recursos de informação e da aplicação dos mesmos de acordo com suas necessidades de poder. O que, de uma forma, ou de outra, tende à construção de uma agenda multilateral para solucionar questões de ordem prática.

Como destacado pela United Nations Institute for Disarmament Research (UNIDIR), apesar de se tratar de cibersegurança e não de ciberguerra,"(...) os elementos de cibersegurança internacional – cooperação na construção da segurança doméstica, a expansão de capacidades militares, e aplicação da lei – apresenta uma

[1] "Military forces are no exception. IT is used to manage military forces – for example, for command and control and for logistics. In addition, modern precision- guided munitions illustrate how the use of IT embedded in weapons systems increases their lethality and reduces the collateral damage associated with the use of such weapons. Movements and actions of military forces can be coordinated through networks that allow information and common pictures of the battlefield to be shared widely". (LIN, 2012, p.516)

agenda robusta para o trabalho multilateral"[2]. Nesse sentido, a própria noção de defesa (e segurança) ganha novos contornos. O princípio da defesa reconquista uma projeção que foi, de certa forma, relegada a partir do período pós-Guerra Fria, orientando-se sob novos princípios, principalmente a partir dos atentados de 11 de setembro de 2001, nos Estados Unidos (EUA). Desses eventos resultou o Ato Patriótico, no governo de George W. Bush, como um conjunto de normas para o enfrentamento de qualquer ameaça sentida, ou percebida, contra a segurança nacional norteamericana. Os EUA, como única potência global, passaram a investir em novos armamentos e em ações de informação relacionados à vigilância, à espionagem, e para suprimir protestos internamente. Não existindo, por parte dos recentes governos, qualquer preocupação em discernir a defesa militar, portanto contra inimigos de fato, de atividades de monitoramento e controle que atingem direitos de privacidade de indivíduos, dentro e fora do território estadunidense. Tendência que foi acompanhada por vários países, potencializando o uso do ciberespaço como recurso de infraestrutura em todas as agências governamentais para a troca de correspondências, para o planejamento estatal, para a gestão de documentos e de sistemas operacionais. E por ser um recurso de infraestrutura, a informação é utilizada como um recurso de poder sistematizado, capaz de fornecer o comando e o controle sobre todas as etapas de processos decisórios num contexto complexo formado por diversos atores estatais e não estatais. Essa perspectiva, principalmente num país como o Brasil, que se caracterizaria como periférico emergente, apresenta algumas implicações éticas justamente pela necessidade imperial de se fazer valer uma política de informação que oriente o investimento técnico-científico para a defesa militar. Portanto, quando se trata de planejamento estratégico, devem-se valorizar os aspectos políticos que dão sentido a esse planejamento e trazem em seu bojo questões sociais e humanas.

A sistematização da informação como recurso de poder para a defesa

Apesar do monitoramento e do controle de cidadãos e grupos políticos, por parte do aparato estatal, não ser algo novo, o arcabouço legal estatuído no Ato Patriótico norteamericano consagra a perspectiva das ameaças difusas, mesmo que imaginárias, além de contemplar recursos de informação[3] para o enfrentamento das mesmas de forma preemptiva. Ou seja, ao menor sinal de perigo, segundo a avaliação da burocracia estatal, deve-se atuar para aniquilação, mais do que para a contenção de potenciais inimigos. Pode-se dizer que essa tendência implica no uso indiscriminado dos recursos de informação como instrumento de controle, e em um processo decisório baseado na supremacia da técnica, numa lógica que valoriza o comando e a obedência em detrimento da Política[4] que, segundo Arendt (2002, p.21), "se baseia na pluralidade dos homens".

O que não quer dizer que não haja propriamente uma definição política (no sentido do desenvolvimento de políticas públicas) de informação voltada para o alcance daqueles objetivos. Pois, mesmo a falta de planejamento é uma opção política. No entanto, o que existe é um estreitamento do espaço para a troca e o debate sobre a lógica, o sentido e os impactos que determinadas decisões impõem sobre a vida social, constituindo-se como uma das questões éticas fundamentais. Implica, portanto, em questões éticas fundamentais no que tange à forma de se fazer política, pois naturaliza as questões sociais e humanas, e os usos de técnicas para o controle do corpo e do espaço sem o consentimento da sociedade. Dentre as questões éticas que precisariam ser levadas em consideração, destacam-se: i) a defesa como recurso usado prioritariamente para a manutenção da paz entre Estados; ii) o uso dos recursos de informação para o monitoramento serem usados exclusivamente para conter comprovadas ameaças externas à sociedade e ao Estado brasileiro; e, iii) utilização de recursos de informação dentro de um modelo cooperativo, preferencialmente para a cobertura de necessidades de defesa de setores críticos entre Estados menos desenvolvidos econômica e tecnologicamente.

[2] "The elements of international cybersecurity—cooperation in building domestic security, the expansion of military capabilities, and law enforcement—present a robust agenda for multilateral work". (UNIDIR 2013, p.4).

[3] Segundo a definição do site do Ministério do Planejamento, Orçamento e Gestão, do governo brasileiro, "Recursos de informação: são tanto os acervos de informações quanto os conjuntos ordenados de procedimentos automatizados de coleta, tratamento e recuperação destas informações". Disponível em: http://www.governoeletronico.gov.br/sisp-conteudo. Acesso em: 02 de agosto de 2013.

[4] Política (com "P" maiúsculo), no sentido conferido por Hannah Arendt, que significa a troca de ideias e experiências entre diferentes, baseada na "pluralidade dos homens".

Muitas das iniciativas para a resolução de questões sociais e humanas, ou mesmo econômicas, vem sendo implementadas sob a égide de uma lógica calcada na precisão técnica. Como se constata, ao destacar que o objetivo fundamental da nação é a busca da segurança, efetiva-se uma série de ações pautadas pela burocracia militar. Nesse sentido, processos de tomada de decisão que deveriam passar por processos formais democráticos, contando com a participação popular, de acordo com o princípio da pluralidade, de Arendt (2002), são realizados através de decisões de cúpula, como na guerra ao terror, com as invasões do Afeganistão, em 2001 e do Iraque, em 2003, e as investidas estadunidenses na guerra contra o narcotráfico em território sul-americano, como no caso do Plano Colômbia e das construções de bases militares no Peru e no Paraguai.

No contexto brasileiro, essa tendência de uso de recursos de informação como recursos informáticos para o monitoramento e o controle também é uma realidade, tanto no âmbito nacional quanto no internacional. Todavia, sucessivos governos, principalmente em períodos ditatoriais utilizaram-se daqueles recursos para a segurança interna, mais do que para a dissuasão de potenciais inimigos externos. O que se justificou por dois motivos: o primeiro, pelo Brasil se enquadrar como um país periférico no sistema de poder internacional, não apurando a percepção para importantes ameaças externas, também por causa de governos subjugados aos poderes hegemônicos internacionais; e segundo, por causa da percepção que aqueles governos nutriam pelas ameaças de grupos internos que contestavam os regimes políticos vigentes.

O golpe militar de 1964 foi marcante nesse sentido, impulsionado pela criação do Serviço Nacional de Informação (SNI), que teve como objetivo supervisionar e coordenar as atividades de informações e contrainformações no Brasil e no exterior. O SNI foi substituído, em 1999, pela Agência Brasileira de Inteligência (Abin), com menos força e um papel aparentemente secundário no sistema de defesa nacional. Atualmente, mesmo com o Brasil ganhando maior vulto no cenário político internacional, inclusive como referência no uso das Tecnologias da Informação e da Comunicação (TIC) nas mais diferentes áreas, a tecnologia de monitoramento e controle na área de defesa ainda se apresenta em estágio embrionário e de forma descoordenada.

Entretanto, pode-se dizer que ainda existe espaço para a realização de uma alternativa política que leve em consideração a troca cooperativa e, com isso, a possibilidade de mitigar o "rolo compressor" da lógica técnico-científica imposta pelos países centrais. Nesse sentido, em uma perspectiva que objetiva a proteção da infraestrutura crítica e das riquezas naturais brasileiras (minerais raros, pré-sal etc.), existentes nas plataformas terrestre e marítima atlântica, vislumbra-se fortalecer a defesa militar para tal fim. Considerando essa nova perspectiva, destaca-se, na Estratégia Nacional de Defesa (END)[5] brasileira, o setor cibernético[6] como área na qual devem ser empreendidos esforços para o enfrentamento de ameaças com características difusas, com origem indefinida[7]. Ou seja, dentre outras coisas, explora-se um novo cenário propiciado pelas TIC, considerando estratégias e táticas operadas no ciberespaço, sem se descuidar das relações políticas a serem desenvolvidas de forma multilateral. Nesse sentido, ao integrar sistemas de informação da administração pública, rearranjando a máquina estatal e promovendo a governança eletrônica, a ameaça ao monopólio do uso da força pelo Estado transmuta-se para o ciberespaço, impondo novos desafios à sua prerrogativa como garantidor da soberania nacional.

As TIC, por suas próprias características, contribuem decisivamente para o planejamento da política de informação, e potencializam as ameaças, colocando a ciberguerra como uma possibilidade. O ciberespaço reposiciona atores estatais e não estatais em torno de objetivos que transcendem o espaço nacional, afetando decisivamente a concepção de soberania e, consequentemente, as questões éticas subjacentes às possíveis

[5]Aprovada pelo Decreto no 6.703, de 18 de dezembro de 2008

[6] De acordo com o conceito estabelecido na END: "Cibernética – Termo que se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC), bem como os sistemas de armas e de vigilância". (CARVALHO, 2011, p. 17).

[7] De acordo com o conceito estabelecido na END: "Defesa Cibernética – Conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética". (CARVALHO, 2011, p.18).

relações estabelecidas em torno da política de informação. Assim, princípios éticos são colocados em questionamento pelo sobrepujamento da técnica sobre a Política, e pelas formas de uso abusivo dos recursos cibernéticos.

Se por um lado, torna-se necessária a cooperação para a resolução de problemas de ordem prática, referentes à ciberguerra, por outro lado, o País precisa manter-se precavido em relação aos atores hegemônicos que, por apresentarem superioridade tecnológica, tendem ao domínio das ações ofensivas de informação em relação aos atores tecnologicamente mais fracos. Portanto, o grande desafio do Brasil é colocar em prática uma estratégia de defesa sob um novo paradigma, que una ao mesmo tempo, o empoderamento dos recursos de informação já desenvolvidos, através do planejamento científico-tecnológico soberano, com a articulação de políticas de cooperação com outros países que tenham a mesma necessidade de defesa do Brasil, limitando ao máximo o acesso de informações estratégicas.

A emergência de sistemas de informação como elemento de comando e controle social teve lugar quando de sua percepção como algo sistematizável, manipulável e mensurável pelo Estado. Ciências de Estado, como a Estatística (Estadística em espanhol), desenvolvem-se sob os auspícios da administração pública, contribuindo para a consolidação de uma tecno-burocracia. Portanto, longe de ser efeito de processo técnico, como resultado de ações passivas e desinteressadas, o desenvolvimento técnico-científico é um processo ideológico, carregado de significado político e social. Estabelece-se, por assim dizer, por meio de regras e normas sob objetivos inerentes à razão de Estado. Um exemplo prático seria o investimento na fabricação de *drones*, seja para o monitoramento e o controle, seja para o ataque efetivo aos potenciais inimigos. Ao optar por ações de ataque e defesa por meio de *drones*, a burocracia responsável pela área de Defesa faz uma opção política pela utilização de uma tecnologia que substitua outros artefatos militares convencionais mais custosos. Isso ocorre levando-se em consideração percepções sociais dos diversos grupos que compõem o ambiente interno da administração pública, a percepção que esses grupos tem da dinâmica social externa à administração pública, assim como das necessidades estruturais e funcionais do aparato burocrático.

Atualmente, as estratégias de defesa enfrentam novos desafios em relação à dinâmica das TIC. O que envolveria preocupações de cunho operacional, como: i) a instrução dos militares para a gestão eficaz e eficiente da informação, consubstanciando sua correta organização, em suas diversas formas; ii) o manuseio de componentes eletrônicos, para operar sistemas e redes de informação e comunicação, até a atuação no campo operacional; e iii) a observação do caráter humanitário, em relação às formas de uso dessas informações pelos Estados. Pois, quando uma informação é compartilhada, ela deixa de ser exclusiva de determinado Estado e passa a ser de uso comum do grupo cooperante. E o problema reside nas seguintes questões: quem a utilizará e como a utilizará, para atingir quais objetivos?

Nisso reside, de certa forma, uma mudança de paradigma que tem início na mudança de postura do Brasil frente aos desafios internacionais. A nova conjuntura política e econômica impõe ao País, dessa maneira, rever prioridades científicas e tecnológicas militares. Algumas delas não tinham importância alguma, como os recursos cibernéticos, e outras já tiveram importância, mas foram relegadas em passado recente, como o investimento em artefatos convencionais (i.e. navios de guerra, blindados, aviões etc.). O que está relacionado diretamente à complexidade que marca a estrutura burocrática estatal e sua necessidade de controlar recursos, planejar programas e projetar poder.

O esforço brasileiro em relação ao controle e ao domínio do ciberespaço confunde-se, de certa forma, com os objetivos traçados pelo Estado para a ocupação do território nacional. Expedições científicas realizadas desde o século XIX, com o objetivo de coletar dados sobre a natureza, a topografia etc., vem sendo parte de uma política de controle sobre tudo o que ocorre e quais seriam as potencialidades oferecidas pelo território brasileiro. Assim, expedições para a implantação das linhas telegráficas, lideradas pelo Marechal Cândido Rondon, por exemplo, demonstram a relevância concedida pelo Estado para a integração e o reconhecimento sobre onde se projeta essa soberania.

Nos anos 1960, concebeu-se o Sistema Brasileiro de Telecomunicações, como a primeira iniciativa no mundo para a construção de um sistema integrado de telecomunicações. Em 1998, o Brasil entra na era do georrefer-

enciamento por satélite para o monitoramento do espaço territorial amazônico, tendo como pilar o pacto cooperativo com os países amazônicos. Pode-se dizer que a concretização de várias ações de informação foram pautadas pela agenda do Tratado e Cooperação Amazônica (TCA), assinado em 1978. Posteriormente, nos anos 1990, implantou-se um sistema de informação para o controle e o monitoramento territorial, que ficou conhecido como Sistema de Vigilância da Amazônia (SIVAM), inserido na macroestrutura do Sistema de Proteção da Amazônia (SIPAM), e objetiva fornecer informação para a tomada de decisão política em várias áreas de atuação de atores públicos estatais e não estatais. Segue-se, no século XXI, a ampliação de uma agenda em política de informação baseada na expansão geoestratégica do Brasil, agora em direção às suas fronteiras marítimas. Surge a necessidade de proteger recursos naturais, antes inexplorados, mas devidamente mapeados pelo Estado brasileiro. Da necessidade política de afirmação de poder, cresce a necessidade de proteção dos recursos por meio de ações de informação em defesa. Agora, além do território amazônico, as preocupações do Brasil voltam-se também para o Oceano Atlântico, denominado "Amazônia Azul" pela Marinha de Guerra do Brasil.

Essa linha do tempo demonstra o quanto torna-se necessária à estratégia de defesa, a articulação de uma política de informação que leve em consideração o contexto geopolítico e os atores envolvidos, e a partir disso, o desenvolvimento de uma arquitetura dos recursos de informação que serão capazes de responder aos desafios impostos pelas relações internacionais. Atualmente, a descoberta do pré-sal e a liderança política exercida pelo Brasil de forma direta na América Latina (AL), por meio do Mercosul e da Unasul, e entre os países considerados emergentes, por meio do G-20 e dos BRICs, são eventos que contribuem para a projeção do País no cenário internacional. Essa realidade retroalimenta-se por meio do histórico papel que o Brasil exerce na AL e na África como ator cooperante na área técnico-científica em setores como: agropecuária, informação científica e tecnológica, energia, e segurança e defesa. Esse é um princípio de política externa que o Brasil carrega, e essa preocupação converge para o planejamento da END.

Um dos pontos mais importantes da END encontra-se no investimento em recursos de informação como fortalecimento da estrutura militar em relação à possibilidade da eclosão de uma ciberguerra. Nesse sentido, algumas iniciativas voltam-se para as discussões na área de Defesa, considerando dessa vez o investimento em recursos de informação para a guerra, envolvendo diversos órgãos, por meio de políticas cooperativas com atuação em rede.

Da cooperação política à infraestrutura das redes: a estratégia de informação para a Defesa

Pode-se dizer, de certa maneira, que no âmbito de atuação direta do Brasil sobre a América do Sul e o Atlântico Sul, as condições políticas seriam mais favoráveis para uma cooperação internacional irrestrita com aqueles países que possuem certa afinidade cultural e geográfica. Um exemplo seria o dos mecanismos de cooperação técnica internacional (CTI), na qual o Brasil usufrui de uma posição de fornecedor de *expertise* tecnológica nas áreas de infraestrutura, saúde, agricultura, prospecção geológica etc., por meio de empresas e órgãos estatais. De certa forma, estruturar um sistema de informação, que seja compartilhado, demandaria alguns cuidados estratégicos em se tratando de atores estatais com disparidade em nível tecnológico, mas que seria essencialmente cooperativo. Por outro lado, com relação aos *players* globais, com interesses no Atlântico Sul, como é o caso dos países membros da Organização do Tratado do Atlântico Norte (OTAN), o Brasil pode e deve cooperar, mas tendo a noção exata de que poderá ser uma relação desigual para o País, na qual entraria como potencial consumidor tecnológico. Ou seja, duas perspectivas, e duas formas de estar no mundo por meio dos possíveis usos cooperativos dos recursos operacionais de informação; como considera Amorim (2013): "[...] do ponto de vista regional, na América do Sul, cooperação; do ponto de vista global, dissuasão. Sem perder de vista que também tem que ter cooperação, nada é preto e branco."

Apesar de estar previsto na END a possibilidade de um conflito cibernético, e a adoção de medidas para a defesa militar da infraestrutura crítica, o atual Ministro da Defesa brasileiro, Celso Amorim, reconheceu que o

Brasil não está preparado para enfrentar os desafios impostos pelas ameaças cibernéticas[8]. Tendo em vista a projeção estratégica do País nas regiões amazônica e do Atlântico Sul, torna-se crucial questionar como deverá ser estabelecida a relação política entre os diversos atores com os quais o Brasil se relaciona militarmente para o compartilhamento e o uso das informações. Porque ações de informação preparativas para a ciberguerra, resultam de planejamentos diferentes, para atingir objetivos diferentes. No caso dos fóruns nos quais o Brasil é membro, como o da Unasul, as discussões giram em torno de uma perspectiva cooperativa, em que se valoriza, primordialmente, uma relação horizontalizada. Por outro lado, o Brasil insere-se no sistema político internacional como um ator de peso, transformando-se em alvo de ameaças potenciais.

A mesma necessidade que impulsiona o Brasil para a cooperação irrestrita com seus vizinhos de fronteira, impõe ao País a troca com outros atores hegemônicos, que alimentam outros interesses que não uma relação alicerçada na dialética política mas, estritamente, no mercado competitivo. Portanto, a mesma dinâmica que proporciona a cooperação, produz a ameaça à soberania nacional, acarretando questões éticas fundamentais, como a possibilidade de acesso, sem o consentimento dos órgãos de defesa às informações estratégicas nacionais, como no caso da coleta de dados do Pré-Sal feita pela Agência de Segurança Nacional (NSA, na sigla em inglês), dos Estados Unidos. Segundo González de Gómez (2008, p.4), o que se estabelece na política internacional repercute na política de informação e vice-versa, moldando o que se pode denominar, de "infopolítica". Ou seja, existem questões políticas referentes a um contexto geográfico que, ao se relacionar com o fluxo de informação, com a comunicação e com a cultura, geram determinada situação política. Dependendo da intensidade de utilização de recursos técnicos e dos objetivos traçados politicamente para a execução de ações práticas, tem-se o ambiente propício para o advento de uma ciberguerra.

Essa possibilidade encontra a existência de uma lacuna tecnológica entre os países, causada por profundas desigualdades políticas e econômicas. Essa tendência repercute no arranjo do sistema de poder internacional, em que os Estados mais desenvolvidos apresentam vantagens comparativas inigualáveis em termos técnicos e operacionais em relação aos Estados menos desenvolvidos. Os Estados que dominam a técnica info-comunicacional, e a posicionam de maneira ofensiva, por meio de sofisticados recursos de informação, como satélites, bases de dados, cabos de fibra ótica e até AWACS, podem provocar instabilidades políticas, e gerar confrontos no ciberespaço. Por outro lado, os Estados menos desenvolvidos tecnologicamente apresentam limitações quanto à potência e sofisticação de recursos técnicos, o que compromete as ações de informação a serem implementadas. Por isso, tornar-se-ia ambivalente uma tentativa de cooperação entre países desiguais em termos de poder absoluto, pois os mais fracos, de um modo geral, apresentam elementos motivadores para que fossem, eles mesmos, monitorados e, com isso, um alvo mais fácil para ser atacado.

No caso do Brasil, que é um país considerado emergente, os alvos, apesar de não serem claros, girariam em torno tanto das fontes de riquezas naturais, quanto da projeção de poder do País, com o cenário atual de crescimento econômico sustentável e proatividade no cenário político internacional. Esse parece ser o quadro do Brasil tanto em relação aos Estados Unidos da América (EUA), quanto em relação à China, por exemplo. Essa preocupação torna-se notória quando se torna evidente a atividade de espionagem dos EUA sobre o Brasil, assim como a preocupação da sociedade brasileira em relação às próprias ações de monitoramento do Estado brasileiro contra a própria população. O que já ocorreu em tempo histórico recente e impõe questões relevantes a serem respondidas em outra ocasião.

Algumas delas, como se seguem: a) Como viabilizar um programa de cooperação para a defesa, o que pressupõe compartilhamento de informações, sabendo que um dos países cooperantes pratica ações de espionagem contra o outro?; b) Pode-se considerar que a infraestrutura crítica do Brasil esteja minimamente imune em relação a essas ameaças?; c) Qual seria o amparo legal para a proteção das informações que devem ou não ser compartilhadas?; d) Quais seriam os desdobramentos éticos desse novo modelo de defesa?; Como o Brasil se posiciona nesse novo cenário de ameaças difusas, considerando sua complexidade social, política e geoestratégica? Defende-se, a partir dessas questões, que apesar da hegemonia da perspectiva da técnica sobre a política, o Brasil apresenta novas possibilidades de inserção via cooperação multilateral na área de defesa

[8] No Senado, Celso Amorim admite vulnerabilidades na defesa cibernética. Disponível em: http://g1.globo.com/politica/noticia/2013/07/ministro-da-defesa-admite-vulnerabilidades-na-defesa-cibernetica.html. Acesso em: 12 de julho de 2013.

militar. Tenta-se, com isso, inverter a lógica dominante do Mercado e da competição tecnológica, cedendo espaço ao compartilhamento de informações para a cobertura de necessidades comuns, baseado na valorização da negociação e do diálogo.

Considerações finais

A transversalidade é a marca de ameaças difusas, de origem imprecisa, que operam a partir de estruturas em rede, impactando severamente a segurança do Estado. Ações de grupos terroristas, ou do crime organizado transnacional, utilizam-se das TIC para expandir seus negócios. Inerente a esse processo, encontra-se a reprodução de um modelo de C&T que vem sendo implantado nos laboratórios e aplicados ao redor da aldeia global. Paralelo ao discurso da "liberdade de expressão", encontram-se outros valores que limitam essa liberdade a um grupo fechado de corporações privadas e governos centrais. Recentemente, os resultados de novas invenções tecnológicas, que foram publicadas em jornais de grande circulação, dão conta do desenvolvimento de tecnologias que já fazem parte do rol das tecnologias militares. Diversos projetos vem sendo colocados em prática em universidades pelo mundo, como o de controle de helicóptero com a força do pensamento, da Universidade de Minnesota, ou a tecnologia da invisibilidade, na Universidade de Rochester (Nova York). Baseado nessa tendência, as duas questões éticas subjacentes ao quadro geral apresentado são: i) Quem se beneficiará desses recursos tecnológicos?; e, ii) Como essas tecnologias serão utilizadas? A técnica domina a política e automatiza as relações sociais, colocando o cidadão comum como objeto da ação e não como ator, que demanda necessidades. As invenções tecnológicas que são elaboradas nas universidades e adotadas em projetos militares, impulsionam os mecanismos de controle ideológico sobre os cidadãos, pautados pelas necessidades de grupos ligados à agenda de defesa nacional.

Voltando aos anos 1950, o ex-presidente estadunidense Dwight Eisenhower pronunciou um famoso discurso, no qual enfatizava os perigos impostos à liberdade democrática, pela falta de controle do crescimento de um complexo industrial-militar. Atualmente, o complexo militar proporciona a cooptação da Política (com P maiúsculo), promovendo a desestabilização e a condenação do sistema democrático estabelecido. Os recursos de informação e comunicação há muito vem sendo utilizados não só como ferramentas para a troca, mas também como instrumentos de controle e monitoramento. E com isso nem sempre a privacidade dos cidadãos é respeitada. Nesse sentido, o que mais interessa em relação à utilização dos recursos de comunicação, são as formas de uso da informação.

A defesa nacional é um dever do Estado em relação à proteção de suas infraestruturas e da sociedade contra ameaças externas e internas. No entanto, o modelo de defesa que vem sendo implantado, obedece à uma dinâmica sistêmica baseada nas diretrizes técnicas orientadas em acordos de cúpula, com suporte do complexo industrial-militar. Nesse sentido, a produção técnica se impõe sobre a lógica da Política, reconfigurando o espaço das trocas e complexificando as relações de poder. Ao Brasil, com suas limitações técnicas, cabe reforçar laços políticos multilaterais, primeiramente com seus vizinhos de fronteira (terrestre e marítima), e depois em fóruns globais cooperativos, como, por exemplo, com os outros membros dos BRICs (Rússia, Índia, China e África do Sul), com o objetivo de fortalecer os recursos de informação para mitigar possíveis danos causados por potenciais inimigos à sua infraestrutura crítica.

Essa parece ser uma lógica diferenciada daquela imposta pelos atores hegemônicos, pois se propõe a estabelecer relações políticas entre atores que possuem interesses e necessidades sociais semelhantes. A técnica não é subssumida mas, de certo modo, deve ser relativizada, e colocada sob o guarda-chuva das relações políticas, possibilitando, dessa maneira, contemplar questões éticas fundamentais em relação à ciberguerra. Mesmo que sejam encontradas dificuldades para o controle técnico-operacional dessas ameaças cibernéticas, a política tecida entre os Estados, por meio da cooperação, possibilita identificar essas ameaças, e neutralizá-las pelo uso político da informação em uma estrutura em rede.

References:

Arendt, Hannah. O que é política?(trad.) Reinaldo Guarany. Rio de Janeiro: Bertrand Brasil, 2002, p.240.

Backstrom, A. and Henderson, I. New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues. In: International Review of the Red Cross, Article 36 weapons reviews, v. 94, n. 886, Summer 2012, pp. 483-514.

Carvalho Paulo Sérgio M. de. Desafios Estratégicos para a Segurança e Defesa Cibernética. SAE, Brasília, 2011, p.18. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf*. Acesso em: 07 de agosto de 2013.*

Felipe Néri. No Senado, Celso Amorim admite vulnerabilidades na defesa cibernética. Disponível em: http://g1.globo.com/politica/noticia/2013/07/ministro-da-defesa-admite-vulnerabilidades-na-defesa-cibernetica.html*. Acesso em: 12 de julho de 2013.*

González de Gómez, Nélida e CHICANEL, Marize. A mudança de regimes de informação e as variações tecnológicas. IX ENANCIB, USP: São Paulo, 2008.

Lin, Herbert. Cyber conflict and international humanitarian law. International Review of the Red Cross. Volume 94 Number 886 Summer 2012. p. 515-531.

MINISTÉRIO DO PLANEJAMENTO, ORCAMENTO E GESTÃO. BRASIL. Disponível em: http://www.governo-eletronico.gov.br/sisp-conteudo*. Acesso em: 02 de agosto de 2013.*

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR). The Cyber Index - International Security Trends and Realities. New York/Geneva, 2013.

David Gorr, Wolf J. Schünemann:

Creating a secure cyberspace – Securitization in Internet governance discourses and dispositives in Germany and Russia

Abstract:

This article deals with the phenomenon of securitization in the emerging policy field of Internet governance. In essence, it presents a combination of theoretical reflections preparing the grounds for a comparative analysis of respective discourses and so-called dispositives as well as preliminary findings from such a comparative project. In the following sections we firstly present some theoretical reflections on the structural conditions of Internet regulation in general and the role and relevance of securitization in particular. Secondly, we shed light on how securitization is constructed and how it might affect the build-up process of instruments of Internet regulation. How does securitization happen, how does it work in different societies/states? Which discursive elements can be identified in elites' discourses? And which politico-legal dispositives do emanate from discourse? In a third section we illustrate our reflections with some preliminary findings from a comparison of cybersecurity discourses and dispositives in Germany and Russia.

Agenda:

ISSN 1614-1687

Authors:

David Gorr, M.A.:

- Institute for Social Sciences, Dept. of Political Science, University of Koblenz-Landau, Kaufhausgasse 9, D-76829 Landau
- ☎ + 49 6341 280 38 400

Dr. Wolf J. Schünemann:

- Institute for Political Science, Heidelberg University, Bergheimer Str. 58, D-69115 Heidelberg
- ☎ +49 6221 542860, ✉ wolf.schuenemann@ipw.uni-heidelberg.de , 💻 http://www.uni-heidelberg.de/politikwissenschaften/
- Relevant publications:

  Schünemann, Wolf J.: E-Government und Netzpolitik - eine konzeptionelle Einführung. In: Schünemann, Wolf J./Weiler, Stefan (Hrsg.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos-Verlag 2012. 9-38.

  Schünemann, Wolf J./Zilles, Julia: Die Vermessung der Netzwerkgesellschaft - Internationale Statistiken und Evaluationen als empirische Grundlagen für die vergleichende Forschung. In: Schünemann, Wolf J./Weiler, Stefan (Hrsg.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos-Verlag 2012. 39-69.

In the course of the so-called information revolution that we experience for at least two decades the impact of the Internet on our daily lives has become immense and it has caused dramatic changes in the way we live and communicate. At the same time, the openness of the Internet seems to have an important downside. With regulation lagging behind, it seems to be a dangerous place. In the emerging net political debates, it is sometimes even depicted or perceived as a wild west[1] full of hackers, cybercrooks and sexual predators. As a consequence, political demand for more or less strict national or international regulations of the allegedly borderless space has increased in recent years. In order to fight cybercrime or cyber attacks or even to perform cyber operations themselves (e.g. cyber-espionage) authoritarian as well as democratic states have developed a variety of techniques and have implemented unilateral and/or multilateral strategies. The currently unfolding details on how and to what extent primarily US and British based intelligence services (NSA and GCHQ) monitor online communication all over the world have shown the strong determination of democratic regimes to secure cyberspace. But, however, how do political-administrative authorities in established and defective democracies react to changing patterns of public life? Which narratives and divergent interpretive schemes are observable in the respective elites' discourses that might serve as justifications for Internet regulation or even censorship? In the following sections, we want to deal with these questions, putting our main focus on the discussion and instruments of cybersecurity. Therefore, we firstly have to explain the structural difficulties of effective Internet regulation and we will deal with the question of what is a cyber threat. In our second section we will present the theoretical concept of securitization and give some general illustrations of how it 'works' in the particular context of cyberspace. In the third section we will present some illustrative findings from cybersecurity discourses and dispositives of Germany that is taken as an established and functioning democracy and Russia which is described as a defective democracy at best or even as an authoritarian state. Finally, our reflections will be summed up by a short conclusion.

Internet governance and cyber threats

The wired world and its fragmented socio-political structures

In this section, the basic condition under which the regulation of the Internet necessarily takes place has to be explained: The cyberspace is a global sphere.[2] The Internet as the 'network of networks' since its beginnings has been planned and designed in a global dimension. This becomes obvious in everyday experiences with the *World Wide Web*. Normally, Internet users do not know where the website they easily access from at home is really located, that means: where the server stands that is hosting the website.[3] Also when using *email* the normal user does not know which way through the Internet it takes, how many borders the data package transcends before reaching the mailbox of the recipient. So in essence, the Internet as a technical infrastructure has a transnational or global dimension. In contrast, political-administrative actors that would be responsible for its technical setup, its organization and regulation are stuck to fragmented institutional structures (mostly of the nation state), i.e. political and legal systems, markets, cultures and languages. This can be seen as the basic structural condition or tension under which the broader field of Internet regulation must be examined. When national governments try to regulate or even restrict online communication, they often act in vein because within the transnational system the owners of a website or the providers of server capacity may reside in another country, thus another jurisdiction and do not fall under domestic law.[4] Also, Internet users can easily

[1] The notion is indeed frequently used, see for instance: Andress, Jason/Winterfeld, Steve: Cyber warfare techniques. xx, 4; Lewis, James A./CSIS: Cybersecurity two years later. 4.

[2] Also „Virtual Public Space, VPS", see Schünemann, Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung.

[3] See Beckedahl, Markus/Lüke, Falk: Die digitale Gesellschaft. 67-68. Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. 18.

[4] Cf. Möller, Jan: Rechtsfrei oder recht frei? 312-314; Nye, Joseph S.: Cyber Power. 6.

ISSN 1614-1687

circumvent national rules and restrictions what makes law enforcement potentially ineffective.[5] True, institutions of international governance (e.g. the Internet Governance Forum of the United Nations, IGF) have been established in order to deal with the transnational quality of cyberspace but as in other policy fields, the international governance of the Internet through organizations and regimes is marked by the same weaknesses of institutional complexity, a lack of cohesion, authority and compliance which basically can be traced back to the fundamental structural condition of fragmentation. Additionally, in the concrete field of Internet governance the international community is marked by a rather clear ideological schism between a group of autocratic states that seek to hold control of the Internet because they fear a de-stabilization of their political systems given the free transnational flows of information and on the other hand a group of liberal democracies that at least publicly support these very flows and thus the leading vision of a 'Web of the Free'[6] and criticize governmental control or censorship of Internet content.[7] This is not to say that democratic regimes would deliberately refrain from cyber espionage. The practices of leading intelligence services as NSA and GCHQ which exploited the technical structure of the internet as well as the dominance of US-based technology firms for their own purposes might serve as an illustration for the very opposite. Indeed, this can be seen as a good reason for questioning the alleged link between democratic order and a 'free' internet. However, given the features of world order listed above, we come to a differentiated assumption concerning the range of action nation states have when dealing with the Internet. While it is generally difficult for nation states to control the Internet because of its global dimensions, governments still have some leverage in Internet regulation and they are more or less able and willing to use or misuse this leverage if it fits to their political goals. And indeed, there always have been regimes that have sought – more or less successfully – to hold a control on their 'national Internet' (e.g. China's 'Great Firewall').

What is a cyber threat?

What is considered a cyber threat in the expanding cybersecurity discourses covers a broad range of quite different activities.[8] In order to analyze and understand how societies discuss and try to build a secure cyberspace it seems to be crucial to have a clear concept of what would be a threat to defend against. Scholars from different disciplines (security studies, political science, international law, etc.) have tried to bring some order into the categorical chaos. A fundamental dichotomy can be drawn between cyber exploitation and cyber attack.[9] As cases of exploitation of the network we can understand most incidents of cyber crime and cyber espionage (Internet fraud, identity theft, etc.) that indeed may cause a lot of damage (especially economic losses), but do not affect the functioning of a given network.[10] Also cyber exploitations do not necessarily serve political goals, they are more often committed for economic profit.

Cyber attacks, in contrast, often have political motives and the main objective is to alter or damage computer networks and create dysfunctions of some kind. According to Hathaway et al. as cyber attack can be understood "any action taken to undermine the functions of a computer network for a political or national security purpose".[11] Cyber attacks can take different forms. The most frequent variants are distributed denial of service attacks (DDOS), the defacement of websites, the planting of inaccurate information or the infiltration of a computer network (e.g. through worms and viruses). The incidents of cyber attacks that have increased in

[5] Cf. Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. 26.

[6] The notion "Web of the Free" is borrowed from a New York Times article with this title written by the lawyer Mark A. Shiffrin and the computer scientist Avi Silberschatz. Therein the authors argue for a loose control of the Internet pointing to the technology's origin in the US.

[7] This schism even reflects in the discussion on how to define cyber attacks, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 824-825.

[8] Cf. Carr, Jeffrey: Inside cyber warfare. xiii, 5.

[9] See Nye, Joseph S.: Cyber Power. 11.

[10] Hathaway, Oona A. et al.: The Law of Cyber-Attack. 829.

[11] Ibid. 826.

number during the recent decade are often depicted as cyberwar or cyber terrorism by politicians, security experts and the media.[12] It is absolutely legitimate that many scholars warn of exaggerations and present more careful and objective definitions. Indeed, not many cyber attacks fulfil the criteria of war or terrorism.[13] When a group of individual hackers or script kiddies succeeds in defacing a governmental website or even shutting it down, this is clearly a cyber attack, but is this really a new type of warfare or terrorism? As important as clear answers to this question seem, especially from an international law perspective, given the far reaching consequences of such categorizations in this respect,[14] for the social reality of threat perception and its political effects which vary from one society to the next objective criteria of what is a threat and how it is to be called do not really matter. This latter reflection points to our constructivist perspective on the issue and leads to the main theoretical concept of securitization.

Securitization and cybersecurity

The concept of securitization

The concept of securitization stands central in an approach to international relations (IR) that originally has been developed by the so-called Copenhagen School (CS) and that should widen the focus of classical security studies from a military and state-centred view to a broader range of security issues. Therefore, security in an IR sense is not defined according to objective criteria, e.g. a military attack. In contrast, what makes an incident a threat is the outcome of an intersubjective process. As Buzan, Wæver and De Wilde define it, security "is when an issue is presented as posing an existential threat to a designated referent object".[15] Thus a security issue can be every issue that is perceived and/or successfully depicted as a security issue by societal actors in a given social setting. So, obviously, this is a constructivist approach to security. Its core concept of securitization has its roots in speech act theory (Austin/Searle) and is understood as a performative act: "The process of securitization is what in language theory is called a speech act. It is not interesting as a sign referring to something more real; it is the utterance itself that is the act."[16] Facing the difficulties in conceptualizing a cyber threat mentioned above this approach provides an elegant solution. As analysts of political processes we do not have to cope with the question whether an issue constitutes a real threat or not. A threat is a threat if there is a so-called securitizing actor that presents it as such and if this move is accepted by a legitimating audience. Or as Balzacq puts the fundamental insight of securitization theory: "no issue is essentially a menace. Something becomes a security problem through discursive politics."[17] The most important effect of a successful act of securitization is a justification for extraordinary measures. The issue is moved outside the normal political procedures into an emergency mode in which governmental action beyond given rules that would otherwise bind security actors is required and accepted. That is why the inventors of the concept put securitization in contrast to politicization, thus highlighting its de-politicizing effect.[18]

[12] For the German discussion Gaycken's book that does not belong into an academic context might serve as a good example: Gaycken, Sandro: Cyberwar.

[13] Cf. Lewis, James A./CSIS: Cybersecurity two years later. 2.

[14] The classification of an incidence as an act of war can have meaningful implications as for example the right to self-defense for a state that suffered from such an assault, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 820 u. 841.

[15] Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. 21.

[16] Ibid. 26.

[17] Balzacq, Thierry: A theory of securitization. 1.

[18] Actually they say both: "Although in one sense securitization is a further intensification of politicization (thus usually making an even stronger role for the state), in another sense it is opposed to politicization." Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. 29.

For the empirical study of securitization Buzan, Wæver and De Wilde themselves propose discourse analysis as favoured methodology without giving concrete indications how the analysis should be conducted. Before designing a more concrete method for our study it is important to note that not just discursive practices should be examined but also the more comprehensive *dispositif* which additionally includes non-discursive practices, institutions, tools etc.[19] The further development of securitization theory by Thierry Balzacq takes this direction. Balzacq regards the phenomenon from a sociological-pragmatic rather than a mere language philosophy perspective.[20] This reorientation has the advantage that the social context in which a securitizing move has to resonate is taken into account. Following Balzacq "the success of securitization is contingent upon a perceptive environment" and "the semantic repertoire of security is […] a combination of textual meaning and cultural meaning".[21] Finally, we affiliate to Balzacq's clarification that securitization should not be understood as a self-referential performative but in reality "takes the form of argumentative processes".[22] So our research essentially is a combination of discourse analysis taking arguments as the main interpretive categories and dispositif analysis examining practices and tools of cybersecurity (see section 3).

Cyberspace: A security issue?

The concept of securitization seems particularly suited to understand how cybersecurity agendas have been developed in different societies. Having said this, it makes no wonder that the concept has been applied to the new policy field in a number of works already.[23] A look into the broader conceptual framework of securitization might help to understand how this application is done. Firstly, according to the inventors of the concept a securitization act needs a referent object, thus any collective unit or principle that is said to be existentially threatened. In our case this might be the Internet as technical infrastructure itself or, via the vision of critical infrastructures disturbed or destructed by cyber attacks, it can be our economy, our social system, maybe, most alarmingly, our lives.[24] In a less dramatic vision, it also could be the idea of a *Web of the Free* that is heavily endangered. Secondly, there obviously is a need for a securitizing actor, someone or a group that might serve as legitimate speaker(s) in this field and is listened to by a legitimating audience. This can be politicians, of course, or cyber experts, be it activists or even representatives of firms that sell cybersecurity tools. Finally, in order to understand securitization in the field of cybersecurity it seems particularly important to look at what Buzan, Wæver and De Wilde call facilitating conditions. For, compared to other attacks in international relations, cyber attacks seem to be relatively harmless, judged by an overlook of the incidents known so far.[25] Assaults that would clearly justify classifications as terrorism or even war have been seldom or have not happened at all. On the other hand, in the field of cybersecurity, there are strong facilitating conditions which help explain why securitization is nonetheless successful. Firstly, the Internet is a relatively young phenomenon, which our industrial societies already heavily rely on. There is a particularly high vulnerability even of sovereign states as for example Stuxnet has shown in the case of Iran.[26] Secondly, the majority of users, including many politicians, does not know in detail how this technology works. Thus there is a fundamental combination of dependency and uncertainty that easily breeds diffuse anxieties. Thirdly, the Internet and many Internet applications have been developed for easy usage, while often enough ignoring security concerns which would have made costly

[19] The concept was originally coined by Foucault, see Foucault, Michel: L'ordre du discours.

[20] Cf. Balzacq, Thierry: A theory of securitization.

[21] Ibid. 13, 14.

[22] Ibid. 22.

[23] See for instance Guitton, Clement: Cyber insecurity as a national threat; Thiel, Thorsten: Unendliche Weiten...? Umkämpfte Grenzen im Internet.

[24] Cf. Billo, Charles G./Chang, Welton: Cyber Warfare. 13-14.

[25] Cf. Carr, Jeffrey: Inside cyber warfare. 8; Guitton, Clement: Cyber insecurity as a national threat. 25. For a regularly updated list of incidents see the respective reports of the US-based Center for Strategic & International Studies (CSIS), URL: http://csis.org/publication/cyber-events-2006 (09/14/2013).

[26] A case that is often referred to also by governmental actors in Western democracies in order to illustrate potential cyber threats, see Hathaway, Oona A. et al.: The Law of Cyber-Attack. 884.

upgrades or even the abdication of higher speed and convenience necessary.[27] Finally, in the field of IR, the cyberspace accelerates a development of power diffusion that is observable since the end of the cold war.[28] This is connected to the fact that attribution has become notoriously difficult in cyberspace which gives states and other actors that are engaged in cyber exploitations or attacks a permanent chance of anonymity or as Carr puts it "plausible deniability".[29] While in conventional conflicts, a state mostly could know by whom it has been attacked, this is not at all the case for cyber attacks the origin of which mostly remains unknown. Not knowing where an attack comes from is also likely to increase uncertainty among security actors because under this condition almost any conventional defence strategy seems hopeless.

Empirical findings from Russia and Germany

For the broader empirical research project that we can illustrate in this article only by exhibiting some preliminary findings, we basically use discourse and dispositive analysis, mainly according to the research program called *Sociology of Knowledge Approach to Discourse*, SKAD.[30] According to SKAD, discourse is to be understood as a material manifestation and circulation of knowledge.[31] SKAD is particularly suited to not just examine the global diffusion of concepts, norms and practices but to investigate more closely the fundamental processes of their reception, translation, and transformation in and through specific socio-cultural settings.

As regards the countries selected, we particularly expect instructive similarities and differences that become obvious through a comparative study of net political discourses and practices in a functioning democracy on the one hand – Germany is considered as belonging to this type – and a defective democracy on the other – here Russia can serve as a good example given its autocratic traits. This selection might be justified for the issue of cybersecurity by a look on the "Freedom of the Net Index", developed by the US-based NGO *Freedom House*. According to the collected data, Russia's 70 million Internet users endure only a "partly free" Internet in their country,[32] whereas Germany's 68 million Internet users face "free" conditions.[33] As democratization literature mostly suggests, public discourses on Internet governance and online communication converge around liberal ideas of civic freedoms, causing bottom-up pressure for democratic reforms in autocracies and defective democracies. Scholars of so-called eDemocracy largely tend to an optimistic outlook saying that new forms of online communication are likely to serve as democratization catalysts.[34] Yet, while Internet communication in Germany seems to be very free and the rather hesitant measures of regulation and control by the government have been responded to by open protests (see the domestic debate on "Netzsperren" in the year 2009), the Russian government is still controlling online communication to a much higher degree and protests for a free Internet are often repressed through state forces. Especially the Russian Internet restriction bill, which initially was created as a blacklist of Internet sites with content that is seen as harmful to children, is considered to be used for censorship of online content of a broader kind. Moreover, in international negotiations on Internet governance, Russia positions itself as the leading nation of an international coalition for new governmental powers of Internet regulation, e.g. within the organizational frame of the Shanghai Cooperation.

---

[27] Cf. Lewis, James A./CSIS: Cybersecurity two years later. 2; Nye, Joseph S.: Cyber Power. 5.

[28] Robert Nye has elucidated the phenomenon of power diffusion in cyberspace in a recent article: Nye, Joseph S.: Cyber Power.

[29] Carr, Jeffrey: Inside cyber warfare. 3.

[30] Keller, Reiner: Wissenssoziologische Diskursanalyse.

[31] Ibid. 97. Konersmann, Ralf: Der Philosoph mit der Maske. 80.

[32] Freedom House: Freedom of the Net 2012. Russia.

[33] Freedom House: Freedom of the Net 2012. Germany.

[34] One of the first books that argued in this direction and attracted a lot of attention is: Benkler, Yochai: The wealth of networks. See also: Abbott, Jason: Social media; Bruns, Axel: Blogs, Wikipedia, Second Life and Beyond; Diamond, Larry: The Coming Wave; Shirky, Clay: Here comes everybody; Shirky, Clay: The political power of social media. In: Foreign Affairs 1/2011. 28.

For the pre-studies to present in this article we only analyzed rather small data corpora of governmental documents, interviews of government officials etc. (Germany: 17, Russia: 15). All texts are open source documents. They were chosen according to the fact that they predominantly deal with the topic of cybersecurity. For this article, we concentrated on elite discourses. In the following sections, we present some preliminary findings from the case studies. For each case, we present the most important results of our interpretive work, i.e. the main recurrent elements we identified in the respective discourse. Taken together, they might serve as a prototype of a code book for a more comprehensive qualitative study (1). Then, we describe which institutions and practices, i.e. dispositives have been developed so far (2).

Germany

Germany's cybersecurity discourse – interpretive analysis

In the governmental documents analyzed so far the Internet technology is primarily perceived as a possibility to boost the economy. The elites consider the Internet as a chance in terms of job creation and ensuring further growth and prosperity (*Economic Argument*, EcoA). In addition, the Federal Foreign Office describes the Internet as a political tool leading to a democratization and to a strengthening of civil society (*Democratic Argument*, DemA). In both respects, it is said, Germany has fully benefitted from digital economy and the Internet so far. Yet, the whole society is perceived to be extremely dependent on a reliable and functioning Internet technology. So, not the cyberspace per se, but the technical infrastructure is seen as particularly vulnerable and insecure (*Risk Perception*, RP). Many officials state that the openness and the expansion of the Internet as well as its disorder or even anarchy would facilitate cyber attacks. The interdependence and global dimension of IT infrastructures would even increase the damage of those assaults. Exactly these two elements have been stressed for instance by Udo Helmbrecht, former president of the *Federal Office for Information Security* (BSI), in 2005 already when he concluded that IT security "must be understood as a national task"[35] and they were updated when he later explicitly demanded a security strategy tackling cyber criminality.[36]

Cyber attacks are perceived by the German Government as attacks coming most frequently from terrorists, professional fraudsters, and criminal organisations because those IT attacks are more attractive than conventional attacks.[37] As to concrete external threats, several cyber exploitations attributed to China and the computer worm Stuxnet discovered in 2010 are explicity addressed when it comes to illustrating risk assessment. Referring to Stuxnet the German Government argues that considerable action needs to be taken because "important industrial infrastructures are no longer exempted from targeted IT attacks" (*Complexity Argument*, CompA).[38] Companies, not to mention individual Internet users, are seen to be overstrained as regards their abilities of handling those cyber attacks alone (*Paternalistic Argument*, PatA). After all, it is said, that the dynamic development of the cyberspace poses new risks which can only be managed by a strong state with a flexible cybersecurity strategy in order to cope with new challenges. However, the necessary measures should only be taken under the condition of ensuring the balance of means and ends (*Proportionality Argument*, PropA). Moreover, the measures should not affect the possibilities of the Internet as an economic driver (*Economic Framework Argument*, EFA) and the protection of data privacy should be taken into account as well (*Data Protection Argument*, DPA).

[35] Federal Office for Information Security: The IT-Security Situation in Germany in 2005. 5.

[36] Federal Office for Information Security: Die Lage der IT-Sicherheit in Deutschland 2007. 5.

[37] Cf. Federal Office for Information Security: Nationales Cyber-Abwehrzentrum. 4.

[38] Federal Ministry of the Interior: Cyber Security Strategy for Germany. 3; see also Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE.

Table 1: The building blocks/interpretive schemes of cybersecurity discourse in Germany:

Dimension	Category	Interpretive Scheme
Perception of the Cyberspace	Economic argument (EcoA)	Cyberspace as an economic driver
	Democratic argument (DemA)	Cyberspace as a political tool for liberation and democratisation
		Web of the Free
	Risk Perception (RP)	Internet (technical network) as a vulnerable/insecure structure
		Internet development as a dynamic process, governmental actors lagging behind
		States/societies as highly dependent on Internet technology and thus vulnerable
Challenges	Complexity Argument (CompA)	New quality and complexity of cyberattacks
	Paternalistic Argument (PatA)	State as provider of IT security for overstrained private IT users (companies, individuals, etc.)
Framework for action	Proportionality Argument (PropA)	Balance of means and ends within the securitization process
	Economic Framework Argument (EFA)	Opportunities of the Internet as an economic driver should not be affected
	Data Protection Argument (DPA)	Ensuring the protection of data privacy
Propositions for Action	New Authorities Proposition (NAP)	Establishing new authorities (National Cyber Response Centre, National Cyber Security Council), strengthen law enforcement agencies
	Coordination Proposition (CoP)	Closer coordination based on intensified information sharing at national and international level
	Standardisation Proposition (StP)	Establishing minimum standards, harmonise rules, introducing legal commitments for the business owners of critical infrastructures
	Awareness Promotion Proposition (APP)	Awareness promotion relating to IT security for private IT users

Germany's cybersecurity dispositif – tools, institutions, practices

As regards new tools, institutions and practices that have been established in the policy field, Germany recently adopted measures to secure cyberspace by a "National Cyber Response Centre" which was set up in April 2011 to "optimize operational cooperation between all state authorities and improve the coordination of protection".[39] Under the lead of the BSI, the centre will submit recommendations to the also newly established "National Cyber Security Council"[40] headed by the Federal Commissioner for Information Technology Rogall-Grothe (*New Authorities Proposition*, NAP). Since the main goal of the centre is information sharing, all important authorities

[39] Federal Ministry of the Interior: Cyber Security Strategy for Germany. 8.

[40] The body is composed of representatives from the Federal Chancellery, different federal ministries (Foreign Affairs, Interior, Defence, Economics and Technology, Justice, Finance, Education and Research) as well as representatives of the Federal States/Länder, see ibid. 9.

will be involved and cooperate both directly and indirectly. Apart from the installation of new authorities, the federal government generally seeks to portray itself as a role model as regards cybersecurity by the publication of guidelines and a general framework addressing cyber threats. State agencies shall establish minimum standards, harmonize rules, introduce legal commitments, strengthen law enforcement agencies and promote coordination at national and international level (EU, NATO, United Nations, OECD etc.; *Coordination Proposition*, CoP, *Standardisation Proposition*, StP). As to international relations, the Federal Foreign Office established the International Cyber Policy Coordination Staff in 2011 and announced this summer that it will appoint diplomat Dirk Brengelmann as a Commissioner for International Cyber Policy.[41] Furthermore, state authorities intensify research on IT security, promote further training for personnel and dedicate more resources in order to tackle cyber threats. Also, the Federal Ministry of Economics and Technology has set up a task force on "IT security in industry" in order to support small and medium sized businesses securing their infrastructures. Overall, the state agencies shall promote awareness among private users (businesses and citizens) and provide them with better information and education relating to IT security (*Awareness Promotion Proposition*, APP).

Russia

Russia's cybersecurity discourse – interpretive analysis

Firstly, compared to Germany, it is significant to note that none of the important Russian doctrines and strategy papers does contain the words "cyberspace", "cyber attacks" or "cyber warfare". All relevant documents[42] use instead the term "information security". In order to understand the mind set of the Russian leaders towards cybersecurity it is important to realize that for them information is per se a "valuable asset" which needs to be protected "in times of peace and war".[43] Consequently, cyber attacks are rather seen as a part of information warfare.[44] The same holistic approach is found in the Russian cyber security strategy published in December 2011.[45] According to this strategy, an information war is a conflict between states with the aim to destroy national information systems leading to a destabilization of the social and political situation in a country. As typical of Russian governmental documents it is held in a defensive tone,[46] trying to avoid any description of Russia's offensive capabilities and focussing only on control, prevention and solution of cyber conflicts.

Cyberspace is generally perceived by the Russian Government as something that the state has no control over yet. However, if a state wants to retain its sovereignty, it is argued, it should be also able to regulate and monitor the information sphere. In this sense, oversight over any phenomenon, in this case information technology, is seen as the most natural thing, no matter how difficult the implementation might be (*Sovereignty Argument*, SovA). Unlike German governmental speakers, Russian officials do not fear the economic but rather the political consequences of cyber attacks which might even lead to a potential regime change (*Revolution Argument*, RevA). In this context, officials stress that information manipulation by the West could evoke Orange Revolution-like events in Russia. For this reason they favour the idea that any interference in the internal affairs of a state via the Internet should be forbidden. The officials acknowledge that information technology is affecting all areas of life. Thus, the main concern of the Russian Government is the growing dependency on the

[41] Brengelmann shall act for Germany's interest on Internet governance at the international level. His appointment attracted attention because it was announced in the face of the NSA scandal, see Federal Foreign Office: Commissioner for International Cyber Policy.

[42] For a complete list of documents related to security issues, see http://www.scrf.gov.ru/documents/sections/3/ (09/12/2013). A brief review of the National Security Concept to 2020 is provided by Haas, Marcel de: Medvedev's Security Policy; Schröder, Henning: Russia's National Security Strategy to 2020; Liaropoulos, Adrew/Dimitrakopoulou, Sophia: Russia's National Security Strategy to 2020.

[43] Heickerö, Roland: Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. 4.

[44] Cf. Giles, Keir: Russia and Cyber Security. 70-71.

[45] Ministry of Defence of the Russian Federation: Conceptional Views on the Activity of the Russian Federation Armed Forces in the Information Space.

[46] Cf. Giles, Keir: Russia and Cyber Security. 78.

Internet technology (*Risk Perception*, RP): "The national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase."[47] But not dependency per se, but reliance on Western technology is seen as an even bigger threat to the national security (*Risk Perception*, RP). The Kremlin has recognised the need for action because it admits that the legal and regulatory framework dealing with information security is imperfect, the protection of state secrets and data privacy is deteriorating and the coordination among authorities is insufficient combined with poor budget financing. The fact that the Russian news agencies and mass media are not competitive and still lagging behind Western technology is also a reason why the Government demands immediate solutions (*Poor Conditions Argument*, PCA). However, also the Russian officials state that any measure will only be useful if the balance of interests among the individual, society and the state in the information sphere is respected (*Proportionality Argument*, PropA).

Table 2: Building blocks/interpretive schemes of cybersecurity discourse in Russia

Dimension	**Category**	**Interpretive Scheme**
Perception of the Cyberspace	Sovereignty Argument (SovA)	Cyberspace as a sphere which is not yet controlled by the state, thus endangering national sovereignty
	Risk Perception (RP)	Internet development as a dynamic process, governmental actors lagging behind
		States/societies as highly dependent on "western Internet technology" and thus vulnerable
Challenges	Poor Conditions Argument (PCA)	Failed attempts and poor legal, political and socioeconomic conditions dealing with cybersecurity
	Revolution Argument (RevA)	Cyberspace/online communication as facilitating conditions for insurrection and regime change
		Web of the Free in a negative sense
		Preventing Orange Revolution-like events in Russia
Framework for action	Proportionality Argument (PropA)	Balance of means and ends within the securitization process
Propositions for Action	New Authorities Proposition (NAP)	Establishing special departments and IT security units, strengthen law enforcement agencies
	Coordination Proposition (CoP)	Closer coordination among authorities
	Self-Reliance Proposition (SRP)	Building independent information systems and create Cyrillic Internet domain names
	Global Governance Proposition (GGP)	Establishing global rules of state behaviour in cyberspace
		Negotiating a cyberspace disarmament treaty

Russia's cybersecurity dispositif – tools, institutions, practices

Since 1997, the Russian Criminal Code includes a chapter tackling "Crimes in the Sphere of Computer Information" composed of three articles, "Illegal Accessing of Computer Information" (Art. 272), "Creation, Use, and Dissemination of Harmful Computer Viruses" (Art. 273) and "Violation of Rules for the Operation of Computers,

[47] Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation.

Computer Systems, or Their Networks" (Art. 274). Russia's Internet is generally regulated under the Law on Mass Media (No. 2124-1) because the authorities interpret the Internet as an extension of media space, with the consequence that bloggers and website owners are responsible for their websites' content. Russian politicians have often expressed their ambitions to have an overall control of the Russian cyberspace implementing a Chinese-style filtering method.[48] The government agency *Federal Service of Communications, Information Technology and Mass Media* (abbreviated: Roszomnadzor), established under the jurisdiction of the Ministry of Telecom and Mass Communications in 2008, is responsible for overseeing compliance with the Law on Personal Data (No. 152-FZ) and the Law on Information, Information Technologies and Protection of Information (No. 149-FZ), both passed in 2006. The agency is also currently maintaining the database of websites containing alleged child pornography, drug-related and extremist material. Another important authority is the *Federal Communication Agency* (abbreviated: Rossvyaz), formed in 2008. It deals with providing public services in the sphere of communication and information.

In matters concerning the implementation of security measures the Russian Government is seeking to increase the efficiency and coordination of government administration (*Coordination Proposition*, CoP), set up special departments and units for cybersecurity (*New Authorities Proposition*, NAP) and enhance law enforcement activities of federal executive bodies. Due to the wide dissemination of information technology in all spheres of life, the Russian Government had already initiated the federal program "Electronic Russia" in 2002 in order to establish an overall eGovernment concept.[49] In order to reduce dependency on technology the Kremlin wants to create independent information systems stemmed from Russian Western engineers and inventors (*Self-Reliance Proposition*, SRP). In this context, on several occasions, Medvedev, Putin and other high-rank officials announced plans to establish a Cyrillic Web of Russia parallel to the World Wide Web. Given its fear of interference into internal affairs via the Internet, at the international level the Russian government is a strong supporter of a universal cyber convention including global standards of state behaviour in cyberspace. Together with the members of the Shanghai Cooperation Group it endorsed the 2011 proposal for an International Code of Conduct for Information Security aiming at strengthening state sovereignty in cyberspace (*Global Governance Proposition*, GPP). Russian officials even claim that the absence of an international treaty would lead to a cyberwar arms race, which they seek to avoid by negotiating a cyberspace disarmament treaty as part of the UN framework.

Conclusion

The cyberspace constitutes a vast field of activities that can be perceived as threats by governmental actors. Facing this fact, the concept of securitization has proved to be particularly useful for examining the emergent cybersecurity discourses and dispositives in different countries. As the constructivist approach suggests: What is perceived as a threat is the outcome of an intersubjective process that normally takes place within a given society. Due to a wide range of powerful facilitating conditions explained above cyberspace is particularly prone to securitization despite the fact that the incidents of cyber attacks known so far have been relatively harmless compared to the effects traditional conflicts in international relations can have. In addition, as especially the sociological-pragmatic version of securitization theory chosen for this article leads one to expect: Whether and how an issue is securitized depends on the social context, but therein also on the established institutions and practices within a given security sub-system.

The preliminary findings of our empirical study of cybersecurity discourses and dispositives in Germany and Russia have shown similarities as well as differences. Securitization is evidently present in both cases. Even some arguments for government action are quite similar (see tables 1 and 2). Nevertheless, the fundamental perceptions of the cyberspace and the risks of Internet technology differ significantly, especially regarding the

[48] Cf. Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan: Russia. 215, 218.

[49] It has been replaced by the program "On the Information Society State Programme of the Russian Federation (2011-2020)" (Executive Order No. 1815-r) in 2010. Moreover, the overall "Strategy of the Development of the Information Society in the Russian Federation" from the year 2008 will address the issue in further detail (cf. Security Council of the Russian Federation 2008).

focus either on the stability of the economy (Germany) or the stability of the political system (Russia). This variation is also expressed in the measures that have been taken and institutions that have been established to create a secure cyberspace in each of the cases. It also reflects the fundamental schism mentioned above that regularly comes up in international negotiations on Internet governance. While Russia pursues a state-centrist regulatory approach to combat and overcome cyber threats which are interpreted in a broad sense of information security, seeking to avoid any interference in internal affairs as an expression of national sovereignty, Germany on the other side has adopted "a mediating role" (Bendiek 2012, p. 15), supporting a global codex for government actions in cyberspace but supporting the idea of a *Web of the Free* and thus not showing any fear of free flows of information. Furthermore, Germany seems particularly eager to promote and protect its economy against cyber threats rather than its political regime.

To finally conclude, it is almost needless to say that a lot of further research on the issue needs to be done. This should include an extension of case studies as well as a more in-depth analysis of discourses and dispositives for each case. This article, nonetheless, might serve as an explorative work preparing the path for future studies in this direction.

References

Abbott, Jason: Social media. In: Kersting, Norbert (ed.): Electronic democracy. Leverkusen [u.a.], Barbara Budrich 2012. 77-102.

Andress, Jason/Winterfeld, Steve: Cyber warfare techniques. Tactics and tools for security practitioners. Amsterdam [u.a.], Elsevier Syngress 2011.

Balzacq, Thierry: A theory of securitization. Origins, core assumptions, and variants. In: Balzacq, Thierry (ed.): Securitization Theory. How security problems emerge and dissolve. London [u.a.], Routledge 2011. 1-30.

Beckedahl, Markus/Lüke, Falk: Die digitale Gesellschaft. Netzpolitik, Bürgerrechte und die Machtfrage, München, Deutscher Taschenbuch Verlag 2012.

Benkler, Yochai: The wealth of networks. How social production transforms markets and freedom. New Haven, Conn. [u.a.], Yale University Press 2006.

Billo, Charles G./Chang, Welton: Cyber Warfare. An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS 2004.

Brenner, Susan W.: Cyberthreats. The emerging fault lines of the nation state. New York [u.a.], Oxford University Press 2009.

Bruns, Axel: Blogs, Wikipedia, Second Life and Beyond: From Production to Produsage. New York, Peter Lang 2009.

Bundestag: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. Drucksache 17/5694. 02.05.2011. URL: http://dip21.bundestag.de/dip21/btd/17/056/1705694.pdf (08/08/2013).

Buzan, Barry/Waever, Ole/De Wilde, Jaap: Security: A New Framework for Analysis. Boulder, Lynne Rienner Publishers 1998.

Carr, Jeffrey: Inside cyber warfare. Mapping the cyber underworld. Beijing [u.a.], O'Reilly 2009.

Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan: Russia. In: Deibert, Ronald/Palfrey, John/Rohozinski, Rafal/Zittrain, Jonathan (eds.): Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace. Cambridge, MIT Press 2010. 209-226.

Diamond, Larry: The Coming Wave. In: Journal of Democracy 1/2012. 5-13.

Federal Foreign Office: Commissioner for International Cyber Policy. 2013. URL: http://www.auswaertiges-amt.de/EN/AAmt/Koordinatoren/Cyber-AP/Uebersicht.html (08/16/2013).

Federal Ministry of the Interior: Cyber Security Strategy for Germany. Berlin 2011. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile (07/25/2013).

Federal Office for Information Security: Nationales Cyber-Abwehrzentrum. Cybersicherheit in Deutschland. Präsentation von Hartmut Isselhorst, Bonn 2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Presse/Cybersicherheit-in-Deutschland.pdf?__blob=publicationFile (08/08/2013).

Federal Office for Information Security: Die Lage der IT-Sicherheit in Deutschland 2007. Bonn 2007. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/lagebericht2007_pdf.pdf?__blob=publicationFile (08/10/2013).

Federal Office for Information Security: The IT-Security Situation in Germany in 2005. Bonn 2005. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2005_pdf.pdf?__blob=publicationFile (08/10/2013).

Foucault, Michel: L'ordre du discours. Paris, Gallimard 1971.

Freedom House: Freedom of the Net 2012. Russia – Country Report. 2012. URL: http://www.freedomhouse.org/sites/default/files/Russia%202012.pdf (06/30/2013).

Freedom House: Freedom of the Net 2012. Germany – Country Report. 2012. URL: http://www.freedomhouse.org/sites/default/files/Germany%202012.pdf (06/30/2013).

Gaycken, Sandro: Cyberwar. Das Wettrüsten hat längst begonnen. Vom digitalen Angriff zum realen Ausnahmezustand. München, Goldmann 2012.

Giles, Keir: Russia and Cyber Security. In: Nação e defesa 133/2012. 69-88.

Guitton, Clement: Cyber insecurity as a national threat: overreaction from Germany, France and the UK? In: European Security 1/2013 (Vol. 20). 21-35.

Haas, Marcel de: Medvedev's Security Policy: A Provisional Assessment. In: russian analytical digest 62/2009. 2-5.

Hathaway, Oona A. et al.: The Law of Cyber-Attack. In: California Law Review 4/2012. 817-885.

Heickerö, Roland: Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm, Swedish Defence Research Agency 2010.

Hindman, Matthew Scott: The myth of digital democracy. Princeton, NJ [u.a.], Princeton University Press 2009.

Keller, Reiner: Wissenssoziologische Diskursanalyse. Grundlegung eines Forschungsprogramms. Wiesbaden, VS-Verlag 2008.

Keller, Reiner: Analysing Discourse. An Approach from the Sociology of Knowledge. In: Forum: Qualitative Social Research (FQS) 3/2005, Art. 32.

Konersmann, Ralf: Der Philosoph mit der Maske. Michel Foucaults L'ordre du discours. In: Foucault, Michel; Konersmann, Ralf (ed.): Die Ordnung des Diskurses. Frankfurt am Main, Fischer Taschenbuch Verlag 2007. 51-94.

Lewis, James A./CSIS: Cybersecurity two years later. A report of the CSIS Commission on cybersecurity for the 44th presidency. In: Studies, Center for Strategic & International, Washington, DC 2011.

Lessing, Lawrence: Code: And Other Laws of Cyperspace. New York, Basic Books 1999.

Liaropoulos, Adrew/Dimitrakopoulou, Sophia: Russia's National Security Strategy to 2020: A Great Power in the Making? In: Caucasian Review of International Affairs, 1/2010 (Vol. 4). 35-42.

Ministry of Defence of the Russian Federation: Conceptional Views on the Activity of the Russian Federation Armed Forces in the Information Space. 2011. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (08/20/2013).

Ministry of Foreign Affairs of the Russian Federation: Information Security Doctrine of the Russian Federation. Approved on September 9 2000. URL: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument (08/16/2013).

Möller, Jan: Rechtsfrei oder recht frei? Zur Vereinbarung, Anwendung und Durchsetzung von gesellschaftlichen Konventionen im Internet. In: Schünemann, Wolf J./Weiler, Stefan (eds.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos 2012. 309-320.

Morozov, Evgeny: The Net Delusion: The Dark Side of Internet Freedom. New York, Public Affairs 2011.

Norris, Pippa: Political mobilization and social networks. The example of the Arab spring. In: Kersting, Norbert (ed.): Electronic democracy. Leverkusen [u.a.], Barbara Budrich 2012. 55-76.

Nye, Joseph S.: Cyber Power. In: Nye, Joseph S. (ed.): The Future of Power. New York, Public Affairs 2011.

Schröder, Henning: Russia's National Security Strategy to 2020. In: russian analytical digest 62/2009. 6-10.

Schünemann. Wolf J.: E-Government und Netzpolitik – eine konzeptionelle Einführung. In: Schünemann, Wolf J./Weiler, Stefan (eds.): E-Government und Netzpolitik im europäischen Vergleich. Baden-Baden, Nomos. 9-38.

Shiffrin, Mark A./Silberschatz, Avi: Web of the Free. In: New York Times, Oct. 23, 2005.

Shirky, Clay: Here comes everybody: the power of organizing without organizations, New York, NY [u.a.], Penguin 2008.

Shirky, Clay: The political power of social media. In: Foreign Affairs 1/2011. 28.

Thiel, Thorsten: Unendliche Weiten...? Umkämpfte Grenzen im Internet. In: INDES 4/2012. 61-67.

Wu, Tim: The Master Switch: The Rise and Fall of Information Empires. New York, Knopf 2010.

Zittrain, Jonathan: The Future of the Internet And How to Stop it. New Haven, Yale University Press 2008.