Ref # 2014011TSD

# European Centre for Information Policy & Security©


December 9

2013

## Surveillance and Monitoring Technology Solutions: Trends, Risks and Effectiveness

## CYBERPOL


*By Lea Hricikova, LL.M-*
*Vrije Universiteit Amsterdam LLM Law and Politics of International Security for CYBERPOL*
European Centre for Information Policy and Security (ECIPS)
3rd Floor ,207 Regent Street LondonW1B 3HH
United Kingdom
T + 44 709 218 4991
F + 44 709 218 4991

**Abstract:**

*Despite the spreading concerns for online privacy and freedom of expression, governments continue their surveillance and monitoring efforts, facing criticism, threats and attacks. The contested legitimacy and the effectiveness of remote monitoring solutions lead to a number of controversies. Market solution for surveillance technology is one of them. It contributed to the current market failure of a secure cyber space, since collecting intelligence, surveillance and monitoring enabled by the technological solutions available on the market has been prioritized over internet security. In addition, the NSA showcase indicates that the voluminous data collected via the technology yields little effective results. Whether the intelligence agencies make an effective use of that data depends on their organizational preparedness as well as on the conditions provided by the government. Yet, the presence of "governance gaps" further deteriorates the security and undermines the intelligence agencies' efforts. Ad hoc decisions with respect to the intelligence communities are persistent, while a common political interpretation of the security environment is missing. The change resides within the security governance and legal refocus on the protection of individuals and their privacy, which can not only tender the exposure and abuse in cyber space but also contribute toward its safety.*

## Introduction:

The public has in 2013 faced that the Tailored Access Operations of USA's National Security Agency (NSA), and other foreign national intelligence programs were not that different from the long-standing practice of Chinese state-sponsored hackers. As concerns for online privacy and freedom of expression spread worldwide, countries continue their surveillance and monitoring efforts. Accompanied by criticism, Indian Government intends to launch its NETRA project for internet surveillance.[i] The surveillance programs mean to make secure the physical as well as the cyber space, which will be the carrier of the collection means for surveillance. Reactions to the surveillance programs varied from warnings against weaponization of the threats, to hacking the Skype's Twitter account by the Syrian Electronic Army in protest against their support to NSA.[ii]

The governmental surveillance and monitoring programs have immediately enveloped into a debate not only on the legitimacy but also on the effectiveness of remote monitoring solutions across cyber space. This debate has highlighted multiple state governance issues regarding the work of intelligence communities. Particularly worrying among those was the controversy surrounding the means of the intelligence agencies' programs, the hardware and software solutions and technologies sold to governments by the private sector businesses. The intelligence communities' penetration into personal data was eased by this technology as well as by many of the communication carriers, who have failed to protect their consumers despite the commonplace belief in their secure infrastructure. Surely, the governmental surveillance and monitoring programs have yielded some results but the overall effectiveness remains dully contested.

Therefore, it is questionable to what extent do the revealed intelligence practices actually provide an advantage for the national defence. This paper aims to identify the obstacles that the intelligence communities face in effort to provide a meaningful monitoring with credible results, that would enable the decision-makers to improve their defence. First, it deals with the means of the intelligence programs focused on surveillance and monitoring in order to draft out the far-reaching importance of the business-to-government market with surveillance equipment for the intelligence community. It also assesses the way in which technology as such impacts the monitoring. The second part draws general conclusions from case study of the NSA's surveillance effectiveness for the defence. The third, and final part, identifies the persisting issues that governments often fall short to provide for the intelligence community: definitions, valid decisions, privacy protection and legal tools.

## i. THE MEANS OF SURVEILLANCE AND MONITORING PROGRAMS

*Acquiring big data with the help of private business*

The capacity to collect the enormous amount of metadata is to an extent predictable within an agency like the NSA, given its statute and its budget. Nonetheless, few would have guessed that the intelligence community came up with a market solution to the challenges of surveillance and monitoring faced in cyber space. A request under the *Freedom of Information Act* led to the release of the NSA's contract with the French company VUPEN made in September 2012 for a 12 months subscription to VUPEN Binary Analysis and Exploits Service.[iii] This allows NSA the access to software backdoors and zero-day exploits. Buying exploits for vulnerabilities became the trend that has spread worldwide to democratic as well as to UN-embargoed regimes.[iv]
The growing list of the customers of the exploits for vulnerabilities has led companies like VUPEN but also the HackingTeam and Netragrad to adopt precautions and trade only with EU-members and NATO-allies. Namely, the debate on exploit trade became so heated that EU considers applying the Dual-Use Regulation, and US and other countries follow.[v] Next to the exploits the vendors offer solutions for lawful interception in deep-packet inspection technology such as webcam-recordings and keystrokes, instant messages, encrypted communication, full access to a skype accounts, remote monitoring of the mobile phone communications as well as handling of the mass recordings. Such technology often includes not only malware but also very complex Trojans, Implants, or Rootkits for backdoor access and target-exploitation.[vi] However, the risk that all of these *lawful* interception technologies end up being used in a country without a rule of law is ubiquitous. Examples of that are the allegations of the French Amesys, or BlueCoat complicity to the crimes of the regimes in (Quaddafi's) Libya, Sudan, Syria or Iran. Therefore, companies progressively incorporate warnings against use for gross violation of human rights when selling the technology.[vii]

Nonetheless, the market relations involve more parties than just state agencies and exploit vendors. Just as the intelligence agencies across the world develop business relationship with the exploit vendors, so do the third parties that technically allow the surveillance of their customers. Google, Microsoft, Mozilla, Facebook or PayPal also buy zero days to fix the bugs in their products. The competitiveness of the market pushes the prices continuously up, with the governmental agencies finding no match in their spending.[viii] This raises the suspicion that the intelligence agencies work toward inserting "intentional flaws" for surveillance's sake into the mentioned third parties' software (which the third parties continuously try to fix). Thus, any intelligence agency risks "prioritizing its own foreign intelligence collection goals over the security of the Internet."[ix]

Since the security of the cyber space might be undermined by the market, it is unsurprising that material motives to hand in exploits operate vulnerabilities market. Thus, one would look long to find an ethical incentive to participate in the market. Creating a price on the exploit (the code) and a value connected with discovering the vulnerability has a direct impact on the intelligence community. Hackers no longer turn in their exploit discoveries to governmental agencies for non-material motives. Thus, the market has removed the "patriotic" effort to warn the military and the critical providers about the deficiencies (still practices in China).[x] In addition to that, the financial motivation has set hurdles to the in-house AntiVirus (AV) research by the third parties as well as any governmental agencies. However, neither the price, not the rising criticism over internet security have contributed to facilitate the exploits in-house as much as the risk of emergence of a black market with exploits for vulnerabilities, thwarting to sell the exclusive code.[xi]

***The indications of sophistication level and mindless collections***

The use of malware and rare vulnerabilities for *lawful* interception seems as an increasingly complex surveillance solution (while many of the companies use open-source code).[xii] However, Jacob Applebaum, who together with *Der Spiegel* presented the technological details of the surveillance program to the public, warns that not all intelligence agencies work with the same (technical) standards. He points out that the technical impression of intelligence agencies should not be directory, and that the lack of sophistication in some case is equally worrying. Simple coding enabling screencapture, while saving screenshots and sending them to the home directory may have critical consequences for investigative journalists in oppressive regimes.[xiii] Kaspersky Lab has last year discovered the "TeamSpy" operation compromising human rights activists and politicians in Eastern Europe and CIS countries. This proved that "not all successful targeted attacks need to build code from scratch."[xiv] In other words, the operation's success does not lie in the complexity of the means used for surveillance anymore.

Nonetheless, the NSA's relies on its sophisticated operations that use passive dragnet surveillance (deep packet inspection), as well as active infections (deep packet injection). Thereby, the communication infrastructure is continuously replaced with interceptors.[xv] Similar infrastructure "ownership" approach is attributed to the China's PLA's 2nd bureau, 3rd department intelligence agency.[xvi] Such approach is not unreasonable, given the effect of connectivity on security. The modernization of infrastructure and communications has been powerful, especially in "cities under stress, marginalized urban and peri-urban populations, high youth unemployment..."[xvii] Arab spring and subsequent development exemplified that the "human networks that allowed information to quickly circulate among urban, peri-urban and rural communities" are a great security concerns. Yet, there is a remarkable difference between the surveillance of the mentioned human networks and between the surveillance of the borderless internet. Thereby, the scale of surveillance and monitoring that the technology enables, not the technical parameters represent the most pressing issue.

The broadness of the surveillance indicates that the intelligence problem that was meant to be resolved is in itself very broad.[xviii] "Defenders must protect everything while attackers need to find only a single vulnerability,"[xix] and targeting the threat is costly and hard.[xx] Since, the *lawful interceptions are* commonplace in democracies scanning for threats to bolster defence in the legally pervasive space surprises no one.[xxi] However, the scale of it raises the suspicion over arbitrary and unconstrained monitoring, and subsequent overload with data and multilingual content, which further obfuscates the detection.[xxii] "Building domain ontology for tagging unstructured data and creating associations between disparate data sources," together with a contextual field investigation are the basis of data collection, to which interception only adds extra comprehensive value.[xxiii] The demand for the very broad targeting which focuses on the elementary functionality of the widely used computer systems, called "soft identifiable targets," has caused the growing insecurity.[xxiv] The more the targeting concerns elementary computer systems – the wider area of users will become vulnerable.

Furthermore, "untargeted" sweeps collect voluminous data without the consent of legal owners (non-US citizens, enabled by Section 702 of FISA Amendment Act). Meanwhile, the interpretation of the extraterritorial jurisdiction used by the *Foreign Intelligence Service Court* (FISC) remains classified.[xxv] But as the voices calling for greater personal security gain on strength, the state, as the ultimate security guarantor, has the prime say. Nonetheless, states have in most case enabled the procurement of the surveillance and monitoring solutions, which stress the "complete and utter market failure in cases of personal security when it is not guaranteed by something bigger."[xxvi] Precisely this issue points out how little relevant is mechanized software to

the resolution of this issue and that the change resides within the security governance and legal refocus on the protection of individuals and their privacy.

## ii. NSA'S EFFECTIVENESS IN COUNTERTERRORISM

The case of NSA surveillance and monitoring has been said to prevent 54 cases of terrorism around the world and save lives.[xxvii] Nonetheless, NSA remains confronted with the justification of the proportion of its surveillance program (and the Section 215 of FISA Amendment Act behind it). While the NSA claims that the data gathered for its counterterrorism intelligence are "the only effective means by which NSA analysts are able continuously to keep track of" terrorist security threats,[xxviii] researchers and a review group proved this effectiveness is questionable.

Of all reactions to NSA's activity, most transformative effect had the Report of the President's Review Group on Intelligence and Communications Technologies (raising 46 ecommendations). It confirmed that the surveillance and monitoring program has reduced neither the risks to public trust, personal privacy, and civil liberty, nor unjustified, unnecessary, or excessive surveillance. Concerns were raised also over the NSA's violation of the FISC legal regime and over the cost-effectiveness of the program.[xxix] Michael Leiter and Benjamin Wittes drew attention to the potential improvements in privacy and transparency stemming from the recommendations but also to the intelligence "cost" they will come at.[xxx] They warned that the checks and balances introduced by the Review Group – such as Oversight Boards, added privacy assessments, and Management and Budget Office controls – when applied unscrupulously, all at once, could transform NSA into an inefficient bureaucracy. Unforeseen security consequences would then be the "cost" of the transformation.

The warnings against NSA becoming a bureaucratically inefficient must be taken seriously, especially since the agency is known as only restricted "by budget or simply by their time" in their pursuit, with "no boundary to what they [NSA] want to do."[xxxi] However, the unconstrained pursuit in a generally pervasive environment that NSA has enjoyed yielded results of little effect, as researches have ascertained. New America Foundation conducted research on "225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11." Their results indicate that investigations in majority of these cases were stimulated by traditional intelligence means, including "the use of informants, tips from local communities, and targeted intelligence operations."[xxxii] These are executed under warrants unrelated to Section 215 or 702. The collected metadata contributed to 4.4 percents of examined terrorism cases under the Section 702, 1.8 percent under the Section 215, and NSA acting under an undefined authority was represented in 1.3 percent of the cases. Thus, the data-collection program results are exaggerated.

The prevalence of the traditional intelligence means in investigation of these cases over the surveillance program highlights the poor information sharing of the existing collection. The New America Foundation research concluded that "the overall problem for U.S. counterterrorism officials is not that they need vaster amounts of information from the bulk surveillance programs, but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement and intelligence techniques."[xxxiii] Thus, while the NSA remains unconstrained, their poor organizational effectiveness, together with mindless collection, did not contribute to the agency's overall efforts as expected. Subsequently, the surveillance and data monitoring program was only vaguely successful in making the intelligence cycle more adaptable and reducing "the window of opportunity presented to potential attackers."[xxxiv]

## iii. GOVERNANCE

The importance of the economic rationale and the market approach, providing the intelligence agencies like NSA with means for surveillance and monitoring is telling of the state security "governance gaps" present. The economic rational has increased the number of stakeholders active in- and aiding to intelligence collection and monitoring in cyber space. Intelligence agencies and states are directly influenced by the security decisions of the industry players.[xxxv] The variety of actors has led to a variety of interpretations on the surveillance and monitoring in cyber space. Therefore, a common political interpretation is needed to address the commercial interest in contrast to the self-regulatory practices in absence of state action of late.[xxxvi]

Without a common political interpretation, the definition of blurred lines between what is a petty crime, what a security threat, and what a hard military attack, and whether the definitions align with state and commercial objectives will remain unidentified. Thus, the elementary question "for the protection of whom the mechanisms are invented" will not be answered (not with regards to needs of end-users).[xxxvii]

Apart from the common political interpretation is for the intelligence community vital also the decision-making of the governments. "The problem with weak security governance is that important decisions are made in an ad hoc manner or not at all because they are deemed someone else's responsibility. Systemic vulnerabilities ensue." For the intelligence community that means that in the event of a cyber-attack, a lack of clearly defined roles, no responsibilities and no processes identified will take place. As seen on the contemporary trend of broad sweeps by the intelligence agencies, the role to decide about security priorities remains, despite its importance, neglected.[xxxviii]

Shall the governments not resolve their environment interpretation and not act on their decision-making – the surveillance and monitoring activities will seriously undermine the privacy development. The current trends point in that direction as well. The privacy debate is interesting with regards to surveillance and monitoring because once the trend of endangering privacy continues, privacy will become a valuable asset.[xxxix] The value (and cost) of privacy is tied with the cost identifying criminals, attackers and terrorists by the intelligence agencies and law enforcement (having privacy is associated with the rising cost of identifying a criminal).

Such cost is dependent not so much on strict governmental resolution on privacy as it is on two factors: firstly, by the possibility of traceability in cyber space, and secondly, by the borderless nature of cyber space, which enables the criminals to become elusive. Thus, privacy is a subject to "good" governance of the two factors and the ability to interpret and make decisions for intelligence agencies.

An additional tool that governments have to their disposal is legislation. Enabling the intelligence agencies to share their data and information collected would not gravely impact on privacy if due process is guaranteed and if the investigative powers are backed by the rule of law. This would restrain the state in overrunning the individual and strengthen the law enforcement with computer forensics available on the local level, which is necessary for effective due process.[xl]

On the international level, Council of Europe has enacted mechanisms for "negative obligations, that is, to refrain from interference with fundamental rights, and positive obligations, that is, to actively protect these rights of states."[xli] Legal tools of this kind are a result of an "alarming development on which the governments turned a blind eye on [and that] has been left up to mostly self-regulatory activities of the IT service providers." For how long can the Council's declaration resist the fast-changing nature of technology used as means for surveillance remains

uncertain. However, legislation as such (as well as its absence) is most indicatory tool of governments' interest and intentions.

## Conclusion:

The market solution for the intelligence community's surveillance technology, software and hardware has changed the way this technology is used, the scale on which is used; it has changed the way stakeholders interact and also the results of the surveillance or monitoring programs. Regardless of how much the intelligence communities pay for the surveillance solutions, or whether they pay at all, a substantial shift toward collecting mindless volume of data and metadata occurred because of the technology. Whether the intelligence agencies make an effective use of that data depends on their organizational preparedness as well as on the conditions provided by the government. Inter-agency and inter-departmental sharing of information might be more useful than the most sophisticated malware for surveillance. A suitable interpretation of the security environment and decision-making contribute to the institutional preparedness during the toughest moments. Additionally, protecting privacy with appropriate legal tools can not only tender the exposure and abuse in cyber space but also contribute toward its safety.

### References :


*Applebaum, Jacob (December 30, 2013). To Protect and Infect: The Militarization of the Internet. Part 2. Chaos Communication Congress, Creative Commons. Available online: http://media.ccc.de/browse/congress/2013/30C3_-_5713_-_en_-_saal_2_-_201312301130_-_to_protect_and_infect_part_2_-_jacob.html [accessed on 17.01.2014]; Paganini, Pierluigi (January 8, 2014). Project NETRA: The Indian Internet Surveillance. Cyber Defence Magazine. Available online: http://www.cyberdefensemagazine.com/project-netra-the-indian-internet-surveillance/#sthash.cRMldVz2.dpuf [accessed on 19.01.2014]*

*ii Cobb, Stephen (October 2013). What Can Big Data Security Learn from the AV Industry. Virus Bulletin 2013 (October 2-4, 2013, Berlin). Available online: http://www.virusbtn.com/conference/vb2013/abstracts/sponsorESET.xml; Paganini, Pierluigi (January 13, 2014). Project Microsoft Hacked by Syrian Electronic Army for Second Time in 2014. Cyber Defence Magazine. Available online: http://www.cyberdefensemagazine.com/microsoft-hacked-by-syrian-electronic-army-for-second-time-in-2014/#!prettyPhoto [accessed on 19.01.2014]*

*iii Responsive Document From National Security Agency to Heather Akers-Healy on Sept. 11, 201; p.4 Available online: https://www.muckrock.com/foi/united-states-of-america-10/vupen-contracts-with-nsa-6593/#787525-responsive-documents*

*iv "Israel, Britain, Russia, India and Brazil are some of the biggest spenders. North Korea is in the market, as are some Middle Eastern intelligence services. Countries in the Asian Pacific, including Malaysia and Singapore, are buying, too, according to the Center for Strategic and International Studies in Washington." In Perlroth, Nicole; Sanger, David, E. (July 13, 2013). Nations Buying as Hackers Sell Flaws in Computer Flaws. New York Times. Available online: http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html?_r=0 [accessed on 19.01.2014]*

*v "VUPEN has promised that the company only will sell its services to NATO countries and will not deal with oppressive regimes." In Kumar, Mohit (September 18, 2013). NSA Bought Hacking Tools from "Vupen", a French Based Zero-Day Exploit Seller. The Hacker News. Available online: **http://thehackernews.com/2013/09/nsa-bought-hacking-tools-from-vupen.html#** [accessed on 19.01.2014]; see also Fidler, David, P. (July 18, 2013). Zero-Sum Game: The Global Market for Software Exploits. Arms Control Law. Available online: **http://armscontrollaw.com/tag/christopher-soghoian/** [accessed on 19.01.2014]; The author implies the possibility of imposing similar regime on the software exploits market as on the arms control. See also Ray, Neil (August 19, 2013). EU Targets Cyber Surveillance Exports and U.S. Considers Cyber Weapon Controls. Global Trade Law Blog. Available online: http://www.globaltradelawblog.com/2013/08/19/eu-targets-cyber-surveillance-exports-and-u-s-considers-cyber-weapon-controls/ [accessed on 19.01.2014]; on the Dutch initiative on the Dual-Use Regulation. The criticism towards the EU approach might be found in Privacy International Report. Chapter: The Purpose of Dual Export Controls. Available online: https://www.privacyinternational.org/reports/our-response-to-eu-consultation-on-legality-of-exporting-surveillance-and-censorship-3[accessed on 19.01.2014]*

*vi Guarnieri, Claudio; Marquis-Boire, Morgan, (December 30, 2013). To Protect and Infect: The Militarization of the Internet. Chaos Communication Congress, Creative Commons. Available online: http://media.ccc.de/browse/congress/2013/30C3_-_5439_-_en_-_saal_1_-_201312292105_-_to_protect_and_infect_-_claudio_guarnieri_-_morgan_marquis-boire.html [accessed on 18.01.2014]; see also Bryant, Chris (July 1, 2013). Europe's Spying Business Thrive Amid Surveillance Uproar. Financial Times. Available online: http://www.ft.com/cms/s/0/d1b47a24-e232-11e2-a7fa-*

*The market solution, together with changes it brings around, allows to identify valuable lessons learned, which might in future help to regulate, if not govern, the cyber space better. Prioritizing first the security of the Internet only after its own foreign intelligence collection goals is the most important lesson. To add up, this effort must be multilateral, "it does not take one state, but all of them to tackle cyber security issues."xlii What matters after all is not the solution to surveillance only – but the philosophy and government attitude that appreciates the solution and brings it forward, alongside with transparency.xliii 00144feabdc0.html#axzz2qrbhe2ag[accessed on 19.01.2014]. See also Perlroth and Sanger, 2013, Supra note iv; The companies include also Netragard in Acton, Mass.; Exodus Intelligence in Austin, Tex.; and ReVuln, Malta; Hacking Team, Milan; Trovicor, Munich; Gamma International, a UK-Germany company; Ultimaco Safeware; Amesys, a French company formerly owned by Bull Group; BlueCoat; and many more.*

*vii Bryant, 2013 Supra note vi; see also Guarnieri and Marquis-Boire, 2013, Supra note vi*

*viii Anon (March 30, 2013). The Digital Arms Trade. The Economist. From the Print Version. Available online: http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade?frsc=dg|a [accessed on 19.01.2014]; see also Perlroth and Sanger, 2013, Supra note iv; see also Subrahmayam, Divya (October 30, 2012). Expert Warns of the Trade in Software Security Exploits. Harvard Law School. Available online: http://www.law.harvard.edu/news/2012/10/30_cybersecurity-soghoian.html [accessed on 19.01.2014]*

*ix Soghoian, Chris (September 13, 2013). How NSA's Cyber Sabotage Puts Us All at Risk . Free Future. Available online: https://www.aclu.org/blog/national-security/how-nsas-cyber-sabotage-puts-us-all-risk [accessed on 19.01.2014]*

*x For the references on the standards in cyberspace in China see Hagestad, William II (October 9, 2013). Operation Middle Kingdom. Secure 2013. Nask and CERT Polska (October 9, 2013, Warsaw). Available online: http://www.youtube.com/watch?v=hCujrWDqCZY [accessed on 17.01.2014]; also see Hagestad, William II (May 11, 2012). Chinese Information Warfare Event. Potomac Institute Cyber Center (May 11, 2012). Available online: http://www.youtube.com/watch?v=h4qlHMJkbs8 [accessed on 17.01.2014]*

*xi Statement of General Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Services (March 12, 2013). Available online: http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander%20testimony%20March%202013.pdf [accessed on 19.01.2014]; p.3*

*xiiGuarnieri and Marquis-Boire, 2013, Supra note vi*

*xiii Applebaum, 2013, Supra note i*

*xiv Kaspersky Security Bulletin 2013. Kaspersky Lab. Available online: http://report.kaspersky.com/ [accessed on 19.01.2014]; also see for hacktivism and for ransomware.*

*xv Applebaum, 2013, Supra note i*

*xvi Guarnieri and Marquis-Boire, 2013, Supra note vi*

*xvii David Kilcullen in Manea, Octavian (November 25, 2013). Future of Warfare in a Post-COIN Conflict Climate. SWJ Discussion with Dr. David Kilcullen . Small Wars Journal. Available online: http://smallwarsjournal.com/jrnl/art/future-of-warfare-in-a-post-coin-conflict-climate [accessed on 19.01.2014]; The full quote: "What I concluded in my research is that there was a strong correlation between a high degree of coastal urbanization and a high degree of unrest in the Arab Spring. I asked myself why is that the case? There are a couple of reasons. One is that all these societies experienced rapid growth of coastal cities in the 20 or 30 years before the uprisings and to some extent, all three cases show a common pattern: cities under stress, marginalized urban and peri-urban populations, high youth unemployment, lack of carrying capacity in a society experiencing significant population growth and urbanization, but at the same time limited economic opportunities. "*

*xviii Clark, Robert, M. (2013, Fourth Edition). Intelligence Analysis: A target-Centric Approach. Sage. London; P.19*

*xix Goel, Sanjay (August 2011). Cyberwarfare: Connecting the Dots in Cyber Intelligence. Communications of the ACM. Vol.54:8. Available online: http://delivery.acm.org/10.1145/1980000/1978569/p132-goel.pdf?ip=130.37.164.140&id=1978569&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF119562FC4B054A7EC2462DD614FE1742D&CFID=284626279&CFTOKEN=75090475&__acm__=1390325707_c67713bab3f9fcb282bfdec679719582 [accessed on 19.01.2014]; p.137*

*xx Florencio, Dinei; Herley, Cormac (no date). Where Do All the Attacks Go? Microsoft Research. Available online: http://research.microsoft.com/pubs/149885/wheredoalltheattacksgo.pdf [accessed on 19.01.2014]; p.11*

*xxi Alexander, General, Keith, B. (July 31, 2013). National Conversation on the Defence of Our Nation and Protecting Civil Liberties and Privacy. Black Hat USA 2013 Keynote. July 27 – August 1. Las Vegas, NV. Available online: https://media.blackhat.com/us-13/us-13-Alexander-keynote.m4v [accessed on 19.01.2014]*

*xxii The program Dishfire indicates to collect up to 200 million SMS Message Components from around the globe, which granted the collectors access to VCARDS, Geocoordinates, SIM Card Changes, Roaming Information, Travel, Financial Transactions, Passwords – found on NSA Dishfire Presentation on Text Message Collection – Key Extracts (January 16, 2014). The Guardian. Available online: http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents?goback=%2Egde_5021173_member_582985855637458947#%21 [accessed on 19.01.2014];; see also Ball, James (January 16, 2014). NSA Collects Millions of text Messages Daily in "Untargeted" Global Sweep. The Guardian. Available online: http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep?goback=%2Egde_5021173_member_582985578319344845 1#%21[accessed on 19.01.2014]; Goel, 2011, Supra Note xix; p.138*

*xxiii Goel, 2011, Supra Note xix; p.137*

*xxiv Meinrath, Sasha in Ricks, Thomas, E. (January 15, 2014). The Future of War (II): As the Nature of War Changes, the Familiar Dividing Lines of Our World are Blurring Across the Board. Foreign Policy. Available online: http://ricks.foreignpolicy.com/posts/2014/01/15/the_future_of_war_ii_as_the_nature_of_war_changes_the_familiar_dividing_lines_of_ou [accessed on 19.01.2014]*

*xxv Axel Arnbak (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013]; see also 50 U.S.C. § 1801(a)(1),(2),(3) and 50 U.S.C. § 1801 in 50 U.S. CODE CHAPTER 36 - FOREIGN INTELLIGENCE SURVEILLANCE, 1978FOREIGN INTELLIGENCE SURVEILLANCE ACT*

*xxvi Ilves, Toomas, Hendrik (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013]; Coney, Lillie (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013]*

*xxvii Statement of General Keith B. Alexander Commander United States Cyber Command before the Senate Committee on Armed Service, 2013, Supra note xi; p.3; see also Bergen, Peter; Cahall, Bailey; Schneider, Emily; Sterman, David (January 2014). Do NSA's Bulk Surveillance Programs Stop Terrorists? New America Foundation. Available online: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf [accessed on 19.01.2014]; Bergen, Peter (January 15, 2014). NSA and Your Phone Records: What Should Obama Do? CNN. Available online: http://edition.cnn.com/2014/01/15/opinion/bergen-nsa-obama-phone/ [accessed on 19.01.2014]*

*xxviii Clarke, Richard, A; Morell, Michael, J.; Stone, Geoffrey, R.; Sunstein, Cass, R.; Swire, Peter (December 12, 2013). Liberty and Security in a Changed World. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies. Available online: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [accessed on 19.01.2014]; p.95;*

*quote from Application Exhibit A, Declaration of [Redacted version] (Dec. 11, 2008). In Re Production of Tangible Things from [Undisclosed Service Provider] (FISC Dec. 12, 2008). Docket Number: BR-08-13*

*xxix The President's Review Group on Intelligence and Communications Technologies, 2013, Supra note xxviii; P.16, 17, 20 and Recommendation 35, 36 on p.229,230; Recommendation 20 on p.173, for the particularities on FISC legal regime see p. 105, 106*

*xxx Leiter, Michael (December 26, 2013). Too Much and Too Little. Lawfare. Available online: http://www.lawfareblog.com/2013/12/too-much-and-too-little/#.Ut8JTdI1jIV [accessed on 19.01.2014]; Wittes. Benjamin (January 13, 2014). Assessing the Review Group Recommendations: Final Thoughts. Lawfare. Available online: http://www.lawfareblog.com/2014/01/assessing-the-review-group-recommendations-final-thoughts/#.Ut8NdtI1jIX [accessed on 19.01.2014]*

*xxxi Applebaum, 2013, Supra note i*

*xxxii Bergen, Cahall, Schneider and Sterman, 2014, Supra note xxvii; see also the infographics on Homegrown Terrorism 2001-2013. Available online: http://natsec.newamerica.net/extremists/analysis [accessed on 19.01.2014]; The investigative methods used identify from 225 terror suspects: 3 to be investigated under NSA 11 surveillance of an unknown authority, 10 under Section 702, 4 under Section 215, 40 because a community tip, 36 because of an informant, 19 because of suspicious activity report, 18 due to other-than-NSA-agency, 12 by routine law enforcement, 62 incidents have unclear investigative methods and 12 were not prevented.*

*xxxiii Bergen, Cahall, Schneider and Sterman, 2014, Supra note xxvii; p.2*

*xxxiv Julisch, Klaus (July 5, 2013). Understanding and Overcoming Cyber Security Anti-Patterns. Computer Networks. Vol. 57:10. Available online: http://www.sciencedirect.com/science/article/pii/S1389128613000388 [accessed on 19.01.2014]*

*xxxv Gercke, Prof. Dr. Marco (**date**). Collective Cyber Defence: A State and Industry Perspective. http://www.ccdcoe.org/cycon/2013/app.html [accessed on 19.01.2014]; see also International Working group on Privacy in Telecommunications Demands Better protection of Privacy – Respect for Context, Transparency and Control Remains Essential. Available Online: http://www.coe.int/t/dghl/standardsetting/DataProtection/News/Web%20tacking.pdf [accessed on 19.01.2014]; the concept of "governance gaps" was introduced by Julisch, 2013, Supra note xxxiv*

*xxxvi Arnbak, 2013, Supra note xxv*

*xxxvii Sophie Int'Veld (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013]*

*xxxviii Julisch, 2013, Supra note xxxiv*

*xxxix Jacobs, Bart (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013]*

*xl Coney, 2013, Supra note xxvi*

*xli Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies (Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies). Available online https://wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM [accessed on 19.01.2014]; para 4; quote from Web Tracking: International Working group on Privacy in Telecommunications Demands Better protection of Privacy – Respect for Context Transparency and Control Remains Essential. Available Online: http://www.coe.int/t/dghl/standardsetting/DataProtection/News/Web%20tacking.pd [accessed on 19.01.2014]f;*

*xlii Oerting, Troels (January, 2013). Building the Digital Fortress: A toolkit for Cyber Security. Computer, Privacy and Data Protection. Reloading Data Protection. 6th International Conference 23-25 January 2013, Brussels. Available online: http://www.youtube.com/watch?v=3yT2tzJGPKA [accessed on 02.08.2013] xliii Ilves, 2013, Supra Note xxvi*