THIS PAPER HAS BEEN PUBLISHED IN Milan SOPÓCI, Mária PETRUFOVÁ, Miroslav ŠKOLNÍK, Viera FRIANOVÁ, Jaroslav NEKORANEC, Lubomír BELAN JIRÁSKOVÁ, Milota KUSTROVÁ, StanislavMORONG (szerk.)

MANAŽMENT - TEÓRIA, VÝUČBA A PRAX 2014: ZBORNÍK PRÍSPEVKOV Z MEDZINÁRODNEJ VEDECKO-ODBORNEJ KONFERENCIE
380 p.
Konferencia helye, ideje: Liptovsky Mikulas, Szlovákia, 2014.09.24-2014.09.26. Liptovsky Mikulas: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2014. pp. 194-201.
(ISBN:978-80-8040-496-3)

SPIES ACT AS A SPY- THE EDWARD SNOWDEN CASE

Péter Bányász
(Péter Bányász, PhD Student at National Univerity of Public Service, Address: H-1101 Budapest, X. Hungária krt. 9-11., Phone: +36 (1) 392-3500 29/457, Fax: +36 (1) 392-3502, 19-400, banyasz.peter@uni-nke.hu)

Abstract: In 2013 the biggest scene was made by an ex CIA and NSA employee, Edward Snowden, which was about the comprehesinve american spying. This document is going to consider the espinoage method of the NSA and its partnerorganisations and their future effects based on all the available information.

Keywords: *NSA, PRISM, surveillance, intelligence*

INTRODUCTORY THOUGHTS

On 6 June 2013 the British *The Guardian* and the American *The Washington Post* dailies announced that the National Security Agency records the telephone calls[1] initiated by the many million subscribers of the telecommunication company Verzion based on the authorization by a court ruling[2] dated 25 April. The novelty in this issue was the creation of the possibility of the almost unlimited collection of data. The collected data included the phone number of the calling and receiving parties, the actual geographical locations of the parties, duration of calls, IMEI identification of phones, the conversations themselves, but the identification of the talking persons was not an objective. Only a few people could suspect at that time, that this report means only the tip of the iceberg in the issue of eavesdropping.

---

[1] GREENWALD, Glenn: NSA collecting phone records of millions of Verizon customers daily, In. The Guardian, 2013. június 6., http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (2013. december 16.).

[2] The authorization was issued by a federal court, called The United States Foreign Intelligence Surveillance Court (hereinafter 'FISC), which is mainly handling the requests for observations deals.

The purpose of this study is to provide a comprehensive interpretation of the eavesdropping issue from the pieces of information obtained by Edward Snowden. The author expects to prove that the issue has political ramifications primarily now after the Echelon scandal 25 years ago, because only quantitative changes occurred in the intelligence community in my opinion, and not qualitative.

The intelligence agencies also adopted themselves to the continuous structural changes of the society, and extended their activities to all imaginable fields.

1. THE GREAT PREDECESSOR

In August 1988 Duncan Campbell published a paper under the title Somebody's Listening[3] with respect to a topic, about which rumours had been in circulation for years: the intelligence agencies of five Anglo-Saxon countries tap and analyse almost all the telecommunication traffic of the world.

The agencies of the five associated states are NSA in the US, Government Communications Headquarters in Great Britain, Communications Security Establishment in Canada, Defense Signals Directorate in Australia and the Government Communications Security Bureau in New Zealand.

The origin of the cooperation could be tracked back to the BRUSA Agreement[4] signed on 13 May 1943, which was not concluded after the emergence of bi-polar world order, but went on existing in the form of UKUSA Treaty as harmonized with the requirements and challenges of the contemporary era. A number of countries indicated their willingness to participate (FDR, South Korea, Norway, Japan) during the years of the cold war, but the cooperation was not extended.

What the Echelon was able to accomplish in the 1980-ies? It could record all the communication in the world conducted with any kind of engineering means, including the deciphering, analysing and evaluation of coded messages. The quantity of data is immense, therefore, predetermined aspects are necessary for the analysis, such as accent, time, key words (bomb, terrorism, Allah, etc.), font set, language, etc.

Besides the concerns about human rights and data protection, the almost unlimited access and automatic monitoring drew the attention to yet another very important aspect. The results of surveillance performed in the interest of national security was often utilized by the political decision makers for business intelligence. As indicated by an investigation[5] conducted by the European Parliament, the information collected by Echelon was used to make transactions worth $US 25-30 billion in the period from 1993 to 2000 (in relation to, among others, satellite systems, aircraft tenders,

---

[3] CAMPBELL, Duncan: Somebody's Listening, In. New Statesman, 1988. augusztus 12., http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf (2013. december 17.).

[4] NSA: UKUSA Agreement Release 1940-1956, In. National Security Agency: Public Information, Declassification and Transparency, http://www.nsa.gov/public_info/declass/ukusa.shtml (2013. december 17.).

[5] European Parliament: Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting, 2001. január 22-23, http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf (2013. december 23.).

telecommunication and chemical projects, power generation, waste processing, etc.), thus ensuring a competitive advantage against the original partners.

2. LEAKING IN THE 21st CENTURY

We cannot ignore the characteristics of the internet generation of the 21st century when discussing the case, according to which the free flow of information is considered equivalent to the essential human rights. This generation does not only objects to any limitation of the internet, but denies the assumption that the interests of national security takes precedence over the essential freedom rights.

The WikiLeaks was initiated in 2006, the face of which is represented by Julien Assange before the public. This site is operated by an international non-profit organisation. which publishes leaked government and other documents, while ensuring[6] unanimity for the sources. One of the most significant case that can be associated with the site was the publication of 700,000 classified and confidential US government documents.

Here are some leaking that can be associated with WikiLeak:

- Confidential documents related to the Scientology Church.
- List of members of a far right British National Party.
- 600 UN documents (partly with confidential qualification).
- Nearly 7000 analyses prepared by the Congressional Research Service, which provides the scientific and research background for the US Congress.
- 92,000 documents related to the war and presence of US in Afghanistan, including many that have been qualified as confidential or secret, as well as top secret.

As can be seen from the above considerations, the appearance of Edward Snowden during the summer of 2013 could not be regarded unexpected entirely. But who is that enigmatic young man after all? Edward Snowden was born on 21 June 1983 in Elizabeth City, North Carolina. His mother used to be the head of computer and administration network of the Federal Court in Baltimore, and his father was an officer of the Coast Guard. He did not graduate from high school, but obtained his equivalent diploma at an evening course General Educational Development (GED), and he attended computer courses in the meantime. In 2004 he volunteered to the military, where he started the training program of special forces, but could not complete the training because of an accident, after which he was discharged. The he worked as a security guard at NSA, then was employed by the CIA as of 2007 in the IT field. He worked as an advisor from 2009 at Dell, as well as at the company Booz Allen, which was considered to be the shadow emporium of the US intelligence activities. He mentioned that he had been inclined to go public with the spy program of NSA, but he believed in the promises of Barack Obama made by him during the election campaign regarding the policy of change, then he was disheartened to see Barack Obama continuing the policy of his predecessor. Based on certain statements, there is reason to believe, that the Russian intelligence noticed him already in 2007.

---

[6] WikiLeaks: What is WikiLeaks? In. WikiLeaks.org, http://wikileaks.org/About.html (2013. december 23.).

He kept on collecting the documents about surveillance. The published documents included the one that Snowden had no access to, but as an IT manager he persuaded his colleagues to give him the necessary passwords, arguing that he needed them as a system manager. In this way he managed to illegally download data from 20-25 colleagues working in the Hawaii regional centre of NSA.

3. THE SNOWDEN CASE

Intelligence agencies soon recognised the potentials of the new technologies.

The PRISM, having a code name SIGAD US-984XN, is a data mining system capable of clandestine surveillance en masse, which is based on the amendment enacted in 2008 of the Foreign Intelligence Surveillance Act issued in 1978, and also on the provisions of the Patriot Act. FISK supervises the legality of surveillance, and gives permission for secrete collection of data. The PRISM is not equal to the governmental supervisory program, it is only one of the nearly two dozens of surveillance systems. According to the leaked documents, PRISM has been used by NSA since 2007.

Considering that large community sites had been in existence at that time only for a couple of years, the agencies proved to be excellent in recognising the potentials of their utilization. The community sites are very useful elements of OSINT. In the contemporary society people tend to spend increasing portions of their days connected to the internet, where they leave plenty of "traces". The majority of users does not care too much about their data and information security, as a result of which interested parties are able to collect substantial mass of information about a targeted person, including preferences, connection network, actual place of staying. The more the people use the given devices, the more accurate the forecast about their future pattern of behaviour could be.

According to my interpretation, the community media are the combination of online means, for which the service providers give the framework only, and the content is produced by the users.[7] The interaction of users constitutes the basis for the community media, which is created by sharing and supplementing the produced content, but it could lead to creating partly or entirely new content too. The applications written for smart phones are also thought to be in the category of community media by the author, because the majority of the applications is based on the interactions by the users, and they have an interactive role among the various community sites.

Based on the slides published by The Guardian, [8] the NSA had access to stored data by means of PRISM, including those of Microsoft since 2007, Yahoo since 2008, Google, Facebook, PalTalk since 2009, YouTube since 2010, Skype, AOL since 2011, Apple since 2012. Large tech companies denied initially that NSA had access to their databases, but information disclosed in August 2013 indicated that NSA paid for the

---

[7] BÁNYÁSZ, Péter: How The Social Media May Be Used To Paralyse The Critical Infrastructure? Economics And Management 2013:(4) pp. 7-14. (2013)

[8] The Guardian: NSA Prism program slides, In. The Guardian, 2013. november 1., http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (2014. január 2.).

coverage of the infrastructure necessary for the surveillance to Microsoft, to Yahoo, as well as to Facebook.

Companies could be enforced to disclose data based on FISA after issuing of court ruling, but the information published by Edward Snowden confirms that NSA collected data in breach of US legislation in a number of cases. With the program XKeyscore they were able to access to all e-mails, chats and browsing history by using personal data. Although the US law prohibits the monitoring of US citizens without permission, but NSA found a mode of data collection with the help of a legal loophole: if a citizen can be associated with an observed foreigner, then data collection is allowed. Internal investigations revealed that the data protection law was violated many thousands of times since 2008, stepping outside the specified field of competence, and the information collected in this way was shared with DEA, as well as with foreign partners services.[9] This was not the only cooperation between NSA and foreign partner organisations. For instance, NSA paid £ 100 million to GCHQ for the help in monitoring the internet.

Information leaked by Edward Snowden dealt not only with the possibility of monitoring e-mails and the full public media, but among others, about:

- Access to ciphered conversations (Skype, Outlook, Hotmail, etc.).
- Analysing habits related to watching adult sites.
- Participation in online strategic games.
- Tapping official and private phones of national leaders.
- Tracking mobile devices all over the world.
- Remotely taking over the control of cameras of mobile devices.
- Inserting "bugs" in IT equipment during shipment that have been ordered through mail, and methods that allow monitoring the IT equipment.
- Eavesdropping on political summit meeting (e.g. G20).
- Tapping the phones of international political organizations (e.g. UN and EU institutions).
- Operations for hacking the above mentioned cryptographic solutions.

The surveillance of network data is now a general practice, most of the intelligence agencies do that, but the USA has an advantage in this respect, because the substantial part of the internet traffic is routed through the US networks also, and most of the data stored in the increasingly used cloud services are in the US server parks. It is possible that the name of the project, PRISM, can be explained by the "scattering" from optical fibres. One should remember that all the data passing through nodes are acquired, as a result of which an immense quantity of data is available for NSA, which has to be analysed, the technological background of which is not know presently. Although a part of data passes through ciphered channels, but NSA and GCHQ managed to hack the SSL technology used for encryption of the internet services. As a result, they gained access to e-mails believed to be secure earlier, and even to health care data and banking information. This kind of encryption is used otherwise by large companies, like Google, Facebook.

NSA intentionally weakened the cryptology standards, and made efforts to propagate cryptology protocols which contained installed backdoors for making their

---

[9] For example the Israeli SIGINT National Unit.

hacking easy. Naturally, this is rather counterproductive, because eventual adverse groups might also recognise the critical points that can be attacked. NSA used bribe, if they could not hack the encryption. One of the largest corporation dealing with IT security installed an algorithm in the product named RSA BSafe for $10 million, which allowed access for NSA.

According to the evidence in the revealed documents, NSA have been regularly monitoring the data of international money traffic, as well as the banking and credit card transaction for years. In a presentation, the targets of surveillance were mentioned as Visa customers in Europe, Near-East and Africa, and the purpose of surveillance was "to collect, store and analyse of transaction data" of leading credit card companies. Spiegel said, that NSA had access to the data of the Brussels based company SWIFT (Society for Worldwide Interbank Financial Telecommunication), that handles the international transfer of money for many thousands of banks. In response to the spying after banking data the EU Committee released warning that the SWIFT agreement might be suspended with regard the US on the ground of violation of legal regulations.

Maybe the tapping and eavesdropping on the leaders of allied countries could be regarded as a reason that has given rise to the greatest furor within the surveillance issue. In October 2013 the main agenda item of the EU summit was the surveillance issue, which swelled into a scandal by then, dealing with the tapping of mobile phones of the European leaders. Angela Merkel and François Hollande made statement denouncing such intelligence activities of the US, which should be primarily interpreted at the level of political communication („Spying is unacceptable between friends").[10] There are, however, considerations of real politics behind the statements, because EU had been in the process of introducing new data protection regulations, one of the most important novelties of which was to prohibit for companies to disclose data of EU citizens to foreign intelligence agencies. It also envisaged the necessity of establishing self contained European digital means (e.g. European Data Cloud), which is independent of the US infrastructure.

It has to be remembered, that Germany has been trying for decades to participate in the UKUSA Agreement. It is my opinion, that the intention of joining the agreement is percolating through the political statements made in relation to surveillance by the country (and indirectly by the entire EU) (see the hearing of Snowden planned by the European Parliament). Lively arguments were generated all over the world by the surveillance practice of NSA. In the meantime, court rulings were issued with different conclusions about the legality of data collection made by NSA. An intermediate federal court declared the data collection through mobile phone made by the National Security Agency (NSA) as unconstitutional, which might lead to a series of lawsuits. As opposed to that, a court in Manhattan evaluated the practice of NSA as legal referring to the 4th Amendment of the Constitution.

In October 2013 Barack Obama announced that he had initiated the control of the oversees operations of NSA, as a result of which the appointed consulting body compiled

---

[10] This statement is particular interest in the light of German surveillance scandal, what popped out in August 2014. Due to this scandal came to light the decades observations of American and Turkish politicians by the Bundesnachrichtendienst, the foreign intelligence agency of Germany.

its recommendations[11] in a 300 page report containing 46 points. Among others, the recommendations included the following items:

- Limiting then abilities of NSA to record phone calls of US citizens in large quantities.
- It is not allowed for NSA to store the obtained data in its own facilities.
- NSA has to seek court permission for making research in the collected data.
- Controlling the intelligence targeted at leaders of friendly countries, and developing the rules for such intelligence.
- Terminating the operation of some spy programs.

In my opinion, the extent of authorized budget is a better way of controlling the surveillance relative to the regulation by law. The US national security agencies have a budget of $ 52.6 billion, from which they can finance the weakening of encryption or the creation of the infrastructure necessary for the surveillance. [12] Although the American public waived lots of rights for the sake of security after 11 September 2001, but the protection of personal data is becoming a primary issue as a result of the leaked information. Formerly the anti-terrorist attitude was prevailing, which meant the unconditional support of the operations by the intelligence services, but recent assessments indicate that an increasing portion of Americans consider the competence of NSA as excessive. This change of paradigm could be a reason why a bill was discussed in the House of Representatives, which could have lead to the reduction of the budget for the Defence Department. Finally, the bill was rejected, but even the submission of such a bill could not have happened before the Snowden case emerged. [13]

CONCLUSION

This study essentially deals with the leaked information related to the American surveillance, but it should be a naiveté to think that other great powers do not perform such kind and so much extensive surveillance on a regular basis. What we know for sure from the Snowden documents is that Germany, France, Sweden and Spain had close cooperation with GCHQ, and developed tools similar to PRISM. These countries usually declare their compliance with democratic principles in the European sense (as opposed to China, North Korea and Russia, for example).

---

[11] SCIUTTO, Jim- PEREZ, Evan: Review: NSA snooping program should stay in place, In. CNN, 2013. december 18., http://edition.cnn.com/2013/12/18/politics/nsa-report/ (2014. január 4.).

[12] GELLMAN, Barton- MILLER, Greg: U.S. spy network's successes, failures and objectives detailed in 'black budget' summary, In. The Washington Post, 2013. augusztus 29., http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (2014. január 4.).

[13] GELLMAN, Barton- MILLER, Greg: U.S. spy network's successes, failures and objectives detailed in 'black budget' summary, In. The Washington Post, 2013. augusztus 29., http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (2014. január 4.).

I think I was able to confirm, that the surveillance made by NSA is not a novelty, it only means that NSA has extended its field of operation utilizing the advanced technologies. The immense amount of data might cause difficulties in the methodology, about the processing and methods of analysing of which we do not have knowledge whatsoever, but presumably NSA found ample solutions for such problems.

The issue has given rise to controversies not only among people in the establishment (even within the same sector), but among the allies of the US and in the public too. I think this issue will not lead to real consequences (except for an eventual more extensive cooperation among the states), and the PRISM, as well as the entire surveillance scandal will gradually fade out and dropped from the headlines, as happened with the Echelon scandal.

REFERENCES

BÁNYÁSZ, Péter: How The Social Media May Be Used To Paralyse The Critical Infrastructure? Economics And Management 2013:(4) pp. 7-14. (2013)

BIOGRAPHY: Edward Snowden, In. Biography.com, http://www.biography.com/people/edward-snowden-21262897?page=1 (2013. december 23.).

BUMP, Philip- OHLHEISER, Abby: The Amash Amendment Fails, Barely, In. The Wire, 2013. július 24., http://www.thewire.com/politics/2013/07/amash-amendment-fails-despite-democratic-support/67584/ (2014. január 4.).

CAMPBELL, Duncan: Somebody's Listening, In. New Statesman, 1988. augusztus 12., http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf (2013. december 17.).

European Parliament: Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting, 2001. január 22-23, http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf (2013. december 23.).

GELLMAN, Barton- MILLER, Greg: U.S. spy network's successes, failures and objectives detailed in 'black budget' summary, In. The Washington Post, 2013. augusztus 29., http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (2014. január 4.).

GREENWALD, Glenn: NSA collecting phone records of millions of Verizon customers daily, In. The Guardian, 2013. június 6., http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (2013. december 16.).

NSA: UKUSA Agreement Release 1940-1956, In. National Security Agency: Public Information, Declassification and Transparency, http://www.nsa.gov/public_info/declass/ukusa.shtml (2013. december 17.).

SCIUTTO, Jim- PEREZ, Evan: Review: NSA snooping program should stay in place, In. CNN, 2013. december 18., http://edition.cnn.com/2013/12/18/politics/nsa-report/ (2014. január 4.).

THE GUARDIAN: NSA Prism program slides, In. The Guardian, 2013. november 1., http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (2014. január 2.).

WIKILEAKS: What is WikiLeaks? In. WikiLeaks.org, http://wikileaks.org/About.html (2013. december 23.).