Čekerevac Z., DSc, Associate Professor,
"Union" University - Faculty of Business and Industrial Management, Belgrade and Business School "Čačak" in Belgrade, Serbia
Dvorak Z., PhD, Professor,
Faculty of Special Engineering of the University of Žilina, Slovakia
Čekerevac P., MSc, Project Manager, Libek – Belgrade, Serbia

INTERNET SAFETY OF SMEs AND E-MAIL PROTECTION IN THE LIGHT OF RECENT REVELATIONS ABOUT ESPIONAGE OF INTERNET COMMUNICATION SYSTEM

Modern business is related to the massive use of electronic communications, electronic cash transactions, credit and debit cards, payments via the Internet, electronic mail transfer, the use of mobile communications and other information technologies. SMEs are virtually unable to carry out their everyday activities without the use of the Internet. However, the many dangers lurk online. Data are vulnerable during their transfer as well as in storage in terms of protection of their integrity and in terms of their secrecy. Extraordinarily rapid development of information technology enables their efficient implementation, but also brings an increased risk of eavesdropping and espionage. "Excess" of capacity allows to attackers to focus their attention not only on the big and important companies, but virtually to all Internet users, including SMEs. This paper discusses the current state of the Internet business, especially the protection of electronic mail. Theme becomes more significant when one considers the recent events related to an affair with tapping internet messages by the NSA, which was revealed by Edward Snowden and published in The Guardian and The Washington Post in June 2013, and have provoked numerous discussions on this topic, which confirmed that many (if not all) states were/are tapping telecommunication's channels, and that the NSA had the "misfortune" to be discovered first.

Introduction. Modern SME businesses are related to a massive use of electronic communications for electronic cash transactions, credit and debit card payments via the Internet, electronic mails transmission, the use of mobile communications and other information technologies. Moreover, modern

business without them practically cannot be realized. Besides a number of benefits, this type of doing business brings many risks because of the possibility of unauthorized access to data by third parties. In addition to be attacked by individuals, Internet users have recently met with the fact that they are monitored and their data are controlled by world most powerful countries government agencies. Various types of Internet users are faced to different types of concerns. Although the vast majority of users think that has nothing to hide, however, hardly anyone feels comfortable at the thought that he/she is the object of one's control. That is why many people decide to pay more attention to protect their communications and their data.

Analysis and presentation of the research. According to the annual report of the European Central Bank (ECB) in respect of non-cash payments in 2011 age there was an increase of 4.6%, to EUR 90.6 billion, compared to the previous year. Credit cards payments included 41% of all transactions. [1] In 2012, the growth of non-cash payment comparing to the previous year was 4.2% and reached EUR 95.5 billion, and credit cards payments have reached 42%. [2]

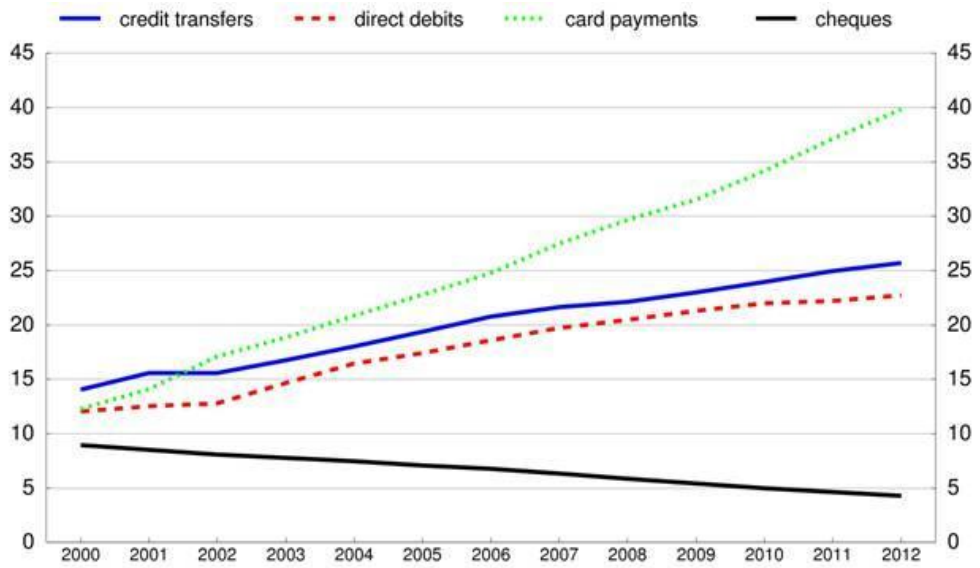

Figure 1 The number of transactions in billions of euros in the period 2000-2012 year (estimated values) Source ECB [2]

According to the Osterman Research [3], 74% of intellectual property of organization resides in electronic mail either as a text or as an attachment. According to the report The Radicati Group Inc. shown in Table 1 it can be seen

that it is estimated that at the end of the year 2013 work little less than four billion e-mail accounts and that this number over the next four years will be increased by over a billion new account. From all accounts, approximately one quarter are accounts used solely for business purposes. It is certain that a large number of private accounts is also used for business purposes.

Table 1 Private and business e-mail accounts from the year 2013 to 2017

	2013	2014	2015	2016	2017
Total number of e-mail accounts in M	**3,899**	**4,116**	**4,353**	**4,626**	**4,920**
Number of business e-mail accounts in M	**929**	**974**	**1,022**	**1,078**	**1,138**
% Business e-mail accounts	24%	24%	23%	23%	23%
Number of private e-mail accounts in M	**2,970**	**3,142**	**3,331**	**3,548**	**3,782**
% Private e-mail accounts	76%	76%	77%	77%	77%

Source [4]

Mobile communications are now very popular, if not the most massive form of communication. The number of active mobile phones will surpass the world population in the year 2014. [5] It is expected that the end of the year 2013 there will be 6.8 billion active cell phones. [6] Based on the statistical data of the World Bank [7] comparing the number of mobile phones per 100 capita list led Macao SAR, China with 284, followed by Hong Kong SAR, China with 228. At the bottom of the list there are Eritrea with 5.4, Somalia 6.7, North Korea 6.9, and Myanmar with 11.1 mobile phones to one hundred capita. Adequate numbers of mobile phones are in the U.S. 98.1, UK 130.75, Serbia 92.8, and in Germany 131.3.

In view of these data it is easy to perceive the wealth of information that is transmitted daily through communication channels. It is certain that there are many interested in collecting data from the communication channels in order of their immediate or postponed use. Every user of the Internet, credit card or mobile phone easily could have guessed that in addition to be a service user at the same time he/she is the object of observation, but there were only a few who were aware of the size and scope of resources of communication espionage. In mid-2013, there suddenly rose up a storm about e-mail, and data circulated by e-mail, security. [8] Although it is believed that the application of a desktop

computers, gateways and encryption make e-mail transmission secure, even in the cloud, Edward Snowden [9] showed that this is not true, that the e-mails, and not only those are actively monitored and eavesdropped. Based on The Guardian serial „On security and liberty“ [10] National Security Agency (NSA) has direct access to systems like Google, Facebook, Apple and other U.S. Internet giants. In strictly confidential document which content is published, NSA access was part of the previously undisclosed program called Prism, which allows the departments to collect material, including browsing history, e-mail contents, file transfer and live chat. The document argues that the data are collecting directly from the servers of major U.S. Internet service providers. The legal basis for the collection of data lies in USA Patriot Act [11], Protect America Act of 2007 [12], Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 [13].

Figure 2 shows some details of data collection by the project Prism.

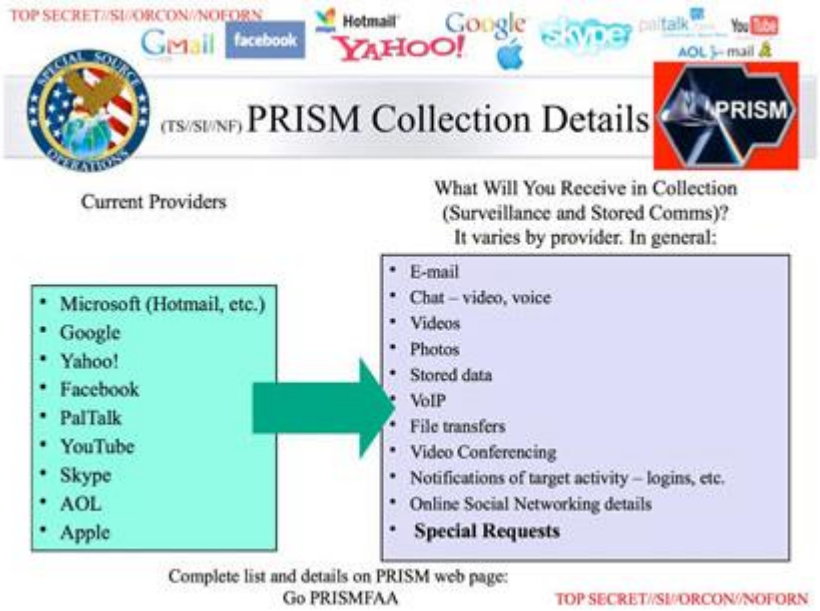

Figure 2 Details of data collection by Prism project (Source: [10])

In accordance with the aforementioned legislation, into the eavesdropping program were gradually included the world's largest internet service providers ranging from Microsoft (2007), via Yahoo (2008), Google, Facebook and PalTalk (2009), YouTube (2010), Skype and AOL (2011), up to Apple (2012). (Source: (Greenwald & MacAskill, 2013)) It is easy to assume that the new

participants in the tapping were not delighted when they received the NSA request for user data takeover, although it was court approved. However, it certainly was nothing compared to the moment when they learned that the NSA, behind their back, secretly took much larger amounts of data. [15] Image released by the Washington Post on 30 October 2013th (see Figure 3) has cast a new light on the extent and type of data collection.

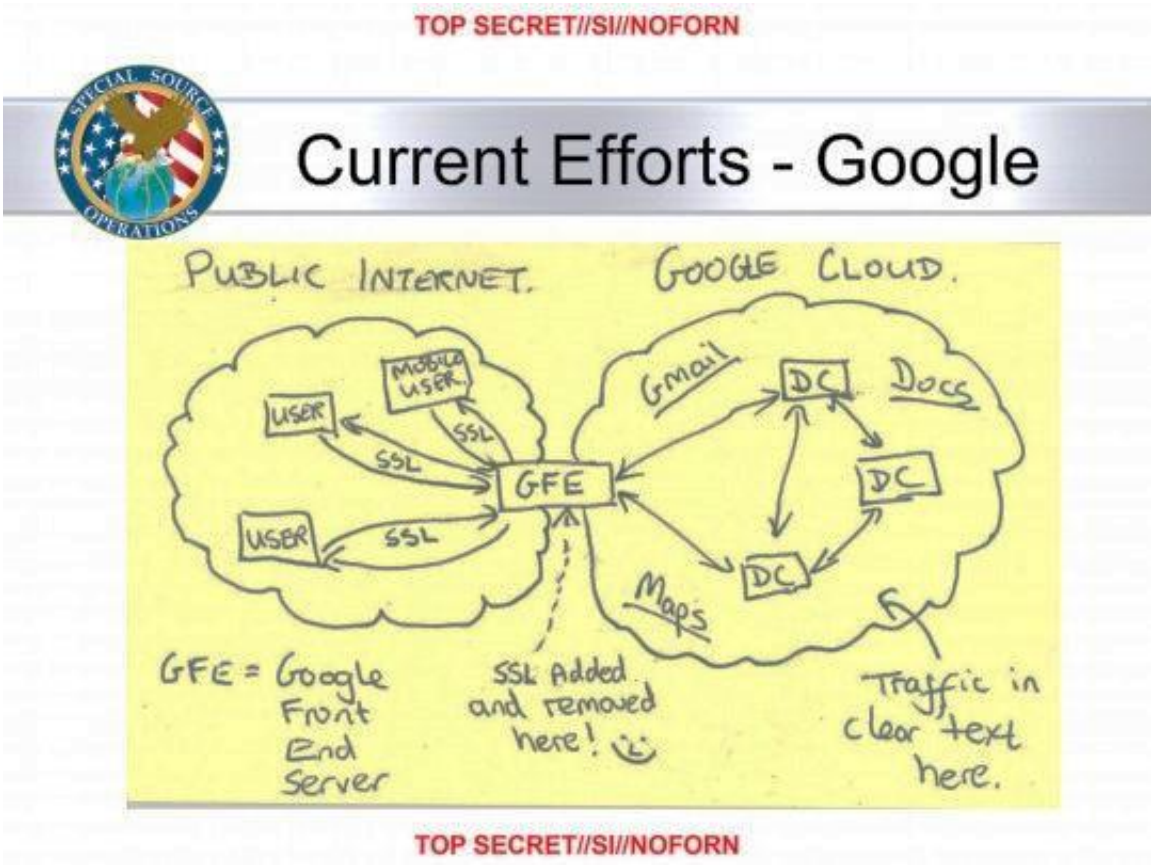

Figure 3 Display of attacks on communications between Google and its users (Source [14]*)*

Based on Figure 3, the claims of Edward Snowden, and so-called well-informed sources, the National Security Agency (NSA) has secretly invaded the links between Yahoo and Google and their clients all over the world. Eavesdropping of these lines the agency was given the opportunity to follow the work of hundreds of millions of user accounts what opened up immense intelligence capabilities. On the basis of confidential information published in The Washington Post [16] activities were carried out within the framework of a secret project "Muscular" intended to intercept traffic from private links

associated with Yahoo and Google's servers. The access point known as the DS-200B is located outside the U.S., at up to now unknown telecommunication service provider(s). It is interesting that into the tapping project is also included the United Kingdom through a joint program "Windstop". At the UK side for the project conducting the General Communications Headquarters (GCHQ) is responsible. This way, bearing in mind that the UK is one of the main centers of (if not the main center) for Internet traffic, these two services, NSA and GCHQ, are able to smoothly follow almost the entire Internet traffic.

However, despite that all the attention is concentrated on tapping and collection of data by U.S. and G.B. intelligence services, there are evidences that the German intelligence service also cooperated with U.S. intelligence agencies, but also with other intelligence agencies. In his statement, the Federal Commissioner for Data Protection Peter Schar has cited by name "Vodafone Deutschland" and "Deutsche Telekom". [17] In June 2013 it was announced that the United Kingdom established its monitoring program ("Tempora") which should outperform the Prism project. [18] It is quite certain that similar projects also exist in other countries, e.g. Italy, India and Canada. [19]

That the situation in this area will not be improved indirectly suggests the statement of Michael Hayden (Director of the NSA from 1995 to 2005) in which he described practically all those who are concerned about the Project Prism and want transparency in the management of the state as "nihilists, anarchists, activists, Lulzsec, Anonymous, twentysomethings who haven't talked to the opposite sex in five or six years". [20] [21]

Protection of emails. Encrypting e-mail today is still not widespread. Most e-mail messages of a typical organization continue to be sent in plain text which allows messages to be easily intercepted. In the year 2013 less than one-half, 44% of organizations provide users the manual encryption, and a little more than a third, 35% have a possibility, depending on the content of the message and the type of data message, to encrypt messages. The situation was even worse in the previous year when the corresponding percentages were 40 and 27. [22]

To ensure encrypted data transfer between the user and the Internet Service Provider (ISP) there should adjust the Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption. SSL connections can be activated in the web browser or email program. Messages can (and should) be encrypted during transmission, but to make it possible, it is necessary to be done at the sender's and also at the recipient's place.

To encrypt e-mail messages functions embedded in the e-mail service can be used, or one can download the software for encryption or client add-ons (such as those using the OpenPGP [23]). In an emergency, can be used Web-based services for e-mail encryption as Sendinc or JumbleMe, although thus forces users to trust a third party, a particular company. [24]

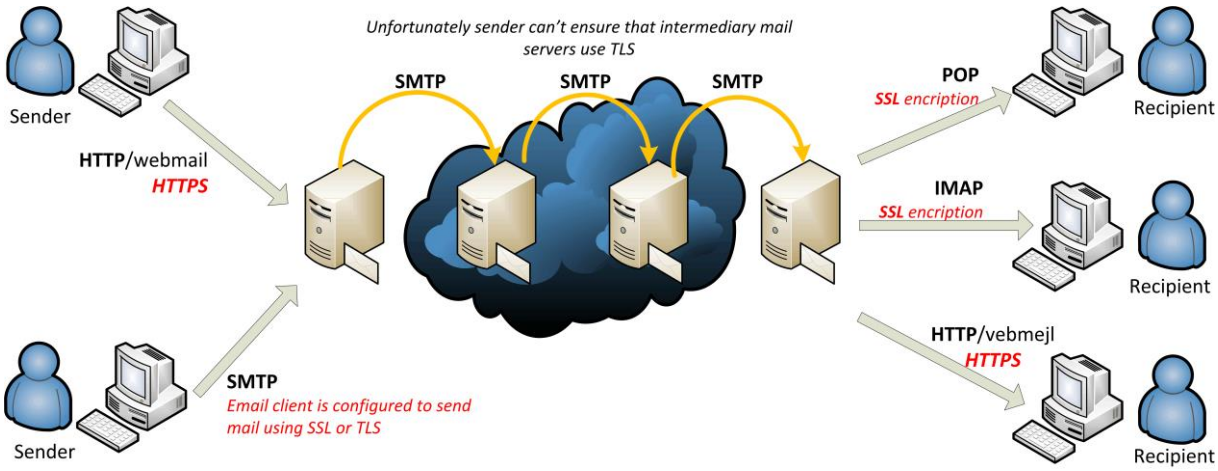

Figure 4 Illustration of a typical electronic mail transmission from a sender to a recipient in versions without encryption (black) and with encryption (grey, italic) (Source: adapted version of the picture published in [8] *and* [25]*)*

Figure 4 shows an illustration of the general case of an e-mail moving from the sender's computer to the recipient's computer, as well as the protocols used at certain stages. Grey (*italic*) indicates possible types of encryption in certain stages. For encrypted mail transfer it is needed that mail sender's server supports SMTP over TLS. As shown in Figure 4, although he has done everything to increase security, the sender cannot influence the route and mode of intermediary mail servers.

The most common forms of data encryption, including S/MIME (Secure / Multipurpose Internet Mail Extensions) and OpenPGP, include installing a

security certificate on the recipient's computer and giving the sender a string of characters, the public key. Many e-mail clients, as well as add-ons for web browsers supports S/MIME standard. Also, it is possible to buy a complete software solution for fully encrypted transmission of messages from the sender to the recipient.

In the case of using portable devices, tablets, notebooks, phones and other mobile devices, to protect e-mail is convenient to use encryption of the downloaded post, but it is more preferably to encrypt the entire device and all data in order to stay them protected in case of the device loss. In addition to the message encrypting, appropriate policies of data deleting should be defined in order to use the available resources rationally.

For email encryption can be used:

- End-to-end encryption,
- Server-server encryption and
- Client-server encryption.

It is certain that the best results can be expected from the end-to-end encryption, so it will be more detailed discussed here.

Encrypting e-mail from end to end, i.e. from the sender to the recipient, it's always been difficult, although the means of achieving this type of encryption are getting better and easier to use. Pretty Good Privacy (PGP) and its cousin free version GNU Privacy Guard (GnuPG) are now standard tools for this purpose. Both of these programs can provide email protection in transit, and also can protect stored data. Major email clients, such as Mozilla Thunderbird and Microsoft Outlook, can be configured to work smoothly with encryption software and allow the sender to sign, verify, encrypt and decrypt e-mail messages with one-click.

Although seemingly simple, the use of GnuPG and/or PGP implies that the sender and recipient use the same software, and it is now rare. If one party does not support GnuPG / PGP no encrypted message transmission from end to end is possible.

The second precondition is that the sender must possess and verify the public keys of recipients to whom the message is intended. It is important that the sender of the message does not fall into the trap known by the name of "man in the middle" when an eavesdropper can induce the sender to use the wrong public key. The man in the middle attack is usually based on curiosity, credulity or inattention of users that their records make available to the attacker, as explained in the work of Srdjan Nikic [26] or for example in works of M. Rouse [27] or, more detailed, J. Admin [28].

Conclusions. Although today's e-business is unthinkable without the internet communications users must be aware of the limitations and risks that it entails. Based on in this work shown analysis, it can be concluded that there is practically no technology that ensures absolute protection of messages and that it is not enough to protect an important message during its travel through cyberspace, but it should be protected from its creation to its reading and archiving. Even in cases of protection "end-to-end" sender sends an encrypted message to the recipient, trusting to the third party, believing that the company that sold the encription software did not instal plug-ins to retrieve the message. In light of the events in connection with Edward Snowden each sender of any message, email or order for payment, must be aware of the risks in electronic communication.

Works cited

[1] European Central Bank, "Payment Statistics for 2011," 10 09 2012. [Online]. Available: http://www.ecb.europa.eu/press/pr/date/2012/html/pr120910.en.html. [Accessed 02 12 2013].

[2] European Central Bank, "Payment statistics for 2012," 19 09 2013. [Online]. Available: http://www.ecb.europa.eu/press/pr/date/2013/html/pr130910.en.html.

[3] Symantec, "Symantec Encryption Solutions for Email, Powered by PGP Technology," Symantec, 13 03 2013. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-solutions-for-email.pdf. [Accessed 01 08 2013].

[4] S. Radicati and J. Levenstein, "Email Statistics Report, 2013-2017," 04

2013. [Online]. Available: http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.

[5] J. Pramis, "Number of mobile phones to exceed world population by 2014," 28 02 2013. [Online]. Available: http://www.digitaltrends.com/mobile/mobile-phone-world-population-2014/.

[6] Betakit, "Number of cell phone plans expected to surpass world's population in early 2014," 29 10 2013. [Online]. Available: http://www.betakit.com/number-of-cell-phone-plans-expected-to-surpass-worlds-population-in-early-2014/.

[7] The World Bank, "Mobile cellular subscriptions (per 100 people)," 2013. [Online]. Available: http://data.worldbank.org/indicator/IT.CEL.SETS.P2.

[8] Z. Čekerevac, P. Čekerevac and J. Vasiljević, "Internet safety of SMEs regarding the security of electronic mail," 07 09 2013. [Online]. Available: http://www.meste.org/fbim/fbim_srpski/FBIM_najava/III_Cekerevac.pdf. [Accessed 19 09 2013].

[9] E. Snowden, "Edward Snowden News," 23 06 2013. [Online]. Available: http://edward-snowden.net/category/edward-snowden/.

[10] G. Greenwald and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others," The Guardian, 07 06 2013.

[11] USA Patriot Act, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001," 24 10 2001. [Online]. Available: http://epic.org/privacy/terrorism/hr3162.html. [Accessed 03 08 2013].

[12] PAA, "Protect America Act of 2007," 05 08 2007. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm.

[13] FISA, "H.R. 6304(110th): FISA Amendments Act of 2008," 09 07 2008. [Online]. Available: https://www.govtrack.us/congress/bills/110/hr6304/text.

[14] B. Gellman, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," 30 10 2013. [Online]. Available: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[15] W. Oremus, "To celebrate spying on Google users, the NSA drew a smiley face," 30 10 2013. [Online]. Available: http://www.slate.com/blogs/future_tense/2013/10/30/nsa_smiley_face_muscular_spying_on_google_yahoo_speaks_volumes_about_agency.html.

[16] The Washington Post, "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," 30 10 2013. [Online]. Available: http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-

google/543/#document/p1/a129319.

[17] T. Jungholt, "FDP-Minister will "Datenuntreue" bestrafen," Die Welt, 03 08 2013.

[18] L. Franceschi-Bicchierai, "Revealed: British Spy Agency Secretly Taps Global Communications," 22 06 2013. [Online]. Available: http://mashable.com/2013/06/21/gchq-spy-agency-taps-global-internet/.

[19] L. Mirani, "Think U.S. Snooping Is Bad? Try Italy, India or Canada," 11 06 2013. [Online]. Available: http://mashable.com/2013/06/11/nsa-privacy-italy-india-canada/.

[20] S. Ackerman, "Former NSA chief warns of cyber-terror attacks if Snowden apprehended," 06 08 2013. [Online]. Available: http://www.theguardian.com/technology/2013/aug/06/nsa-director-cyber-terrorism-snowden.

[21] A. Moore, "Former NSA boss compares PRISM critics to Al Qaeda," 07 08 2013. [Online]. Available: http://www.deathandtaxesmag.com/203430/former-nsa-boss-compares-prism-critics-to-al-qaeda/.

[22] Osterman Research, "Why Should You Encrypt Email and What Happens if You Don't?," 07 2013. [Online]. Available: http://www.ostermanresearch.com/whitepapers/orwp_0194.pdf.

[23] L. Constantin, "OpenPGP JavaScript Implementation Allows Webmail Encryption," 21 11 2011. [Online]. Available: http://www.pcworld.com/article/244406/openpgp_javascript_implementation_allows_webmail_encryption.html.

[24] E. Geier, "How to encrypt your email," 25 04 2012. [Online]. Available: http://www.pcworld.com/article/254338/how_to_encrypt_your_email.html.

[25] Anon, "Email," 01 08 2013. [Online]. Available: https://ssd.eff.org/tech/email.

[26] S. Nikić, "Najčešće metode napada cyber kriminalaca i kako se odbraniti," 05 03 2010. [Online]. Available: http://www.itvestak.org.rs/ziteh_10/zbornik_radova/Nikic%20Srdjan%20-%20Metode%20napada.pdf.

[27] M. Rouse, "Man in the middle attack (fire brigade attack)," 06 2007. [Online]. Available: http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack.

[28] J. Admin, "Man In The Middle Attack Using Ettercap," 2 07 2011. [Online]. Available: http://www.101hacker.com/2011/03/man-in-middle-attack-using-ettercap.html.