COMPARATIVE ANALYSIS OF CYBERATTACKS ON ESTONIA, GEORGIA AND KYRGYZSTAN

Andrzej Kozlowski, MA
University of Lodz, Poland

Abstract

The rapid informatization of the world which has started since the beginning of 90s led to the growing state interdependence from cyberspace. The Internet has become crucial to the society, economy, military of contemporary country. This situation became a new challenge for the national security and more and more often the term cyberwar has been used. Despite the fact that this phenomenon is not clearly defined the massive cyberattack on countries took place in the past.

The main aim of this article is to examine three cases of these attacks: on Estonia in 2007, on Georgia in 2008 and on Kyrygysytan 2009 and to try finding similarities and differences and answer the question who carried out these strikes and why. In order to do it the following factors will be analyzed: the political background of these countries and the relation with the neighbours, the time and scale of attacks and effect of them. In conclusion the article tries to find the most difficult answer who was a perpetrator. The three hypotheses were presented with evaluation of probability of them.

Keywords: Cyberattacks, Russia, Estonia, Georgia, Kyrgyzstan

Growing significance of cyberspace for countries

Since the beginning of 90s the information revolution has begun and the Internet- a tool created to allow communication between universities in the United States, became global. It led to the enormous and rapid increase in number of Internet Users. In 1995 when the measurement started it was 36 million people who accessed to the Internet now this number amounts to approximately 3 billion.[1]

The rapid development of the Internet caused that cyberspace became more and more used by the private companies, authorities of states and average people. A lot of elements of daily life was transferred into the virtual world and things like banking online, voting online became normal in many countries. Also the elements of state critical infrastructure was connected to the Internet and used advantage of it. The information revolution could not omit the military. It allowed them to the access to information in real time. The rapid informatization of the world has changed literally every aspect of life.

The wide spreading of the Internet significantly influences the national security of the states. The cyberspace became a tempting place for the activity of different hackers, groups of cybergangs and cybercriminal and cyberarmies of the countries. The architecture of cyberspace is very favorable for the assailants because when it was created the security was not among priorities. There are certain features which can ease carrying out strike. The potential aggressor is very difficult to trace. Secondly, conducting the hostiles acts in cyberspace is relatively cheap and required only computer with the access to the Internet and hacking skills. The third aspect is time of attack which can be conducted from every corner of the world in seconds. These factors cause that growing informatization of the world led to increasing hostile actions in cyberspace.

In 90s there were mainly attacks carried out by individual hackers who wanted to test its skills and they treated these like a hobby. However, more and more experts start to predict

a forthcoming cyberwar. John Arquilla and David Ronfeld from The American think thank RAND published the "Cyberwar is coming" where they present the theoretical model of potential conflict in cyberspace.[2] When the publication was created it sounded as a science-fiction plot but in 21st century the probability that depicted scenarios will happen significantly has rose up. The cases of Estonia, Georgia and Kyrgyzstan could not be unanimously described as a cyberwar because there is no clear definition of this phenomenon but they represent the examples of massive cyberattacks against the state.

Estonia

Estonia is one of the Baltic Republics which was incorporated to the Soviet Union in 1940. After the dissolution of the Soviet Union Estonia regained independence and started the process of rapid economic, political and social reforms. It joined the European Union and NATO in order to ensure own security. Estonian authorities have seen the gravest threat in Russia and integration with Western structures was the method to overcome it.[3] One of the main strife in bilateral relations was the problem of Russian minority in Estonia which amounts to 26 % of society.[4]

In April 2007 the tensions with Russia significantly increased due to the decision of Estonian capital city – Tallinn authorities, to remove the statue of Bronze Soldier of Tallinn which commemorated the Soviet soldiers who had liberated Estonia. For the Estonians it was a symbol of oppression. For Russians it meant the destroying of the cultural heritage and the lack of respect for the Red Army which fought against Nazi Germans during II World War.[5] After the movement of the Bronze Statue the relationships between Estonia and Russia became very tensed. Kremlin accused Tallinn authorities of breaking human laws and demanded resignation of the Estonian Prime Minister[6]. Simultaneously, the serious riots on the streets between the police and Russian minority in Estonia[7], the protests in front of Estonian Embassy in Moscow[8] and the massive cyberattacks campaign erupted.

Estonia has been highly dependent on the Internet. Almost the whole country was covered by the WiFi Internet, all Government services were available online, 86 % of Estonian populations did banking online. In 2007 there was opportunity to vote electronically and 5,5 % of voters did it.[9]

On 26 April the growing volume of the cyberattacks was noticed and this day is commonly recognized as the beginning of massive cyberattack. The peak of the attack took place on May 9. Since that date the number of hostile acts started to decrease. On May 11 the Paid botnets[10] activity ended, the last attack took place on May 23.[11]

The DDoS[12] attack successfully targeted the websites of all government ministries, two major banks, and several political parties. Hackers were even able to disable the parliamentary email server and disabled the credits cards and automatic teller machines.[13] One of the Estonian banks which was a victim of cyberattack estimated losses around $ 1 million in damages.[14] However, when the ultimately losses were evaluated surprisingly the damages done by cyberattacks were relatively low.[15]

The majority of these attacks were DDoS attacks. It was not a completely new technique, in past there were a lot of incidents using DDoS.[16] However, in Estonia there was an interesting composition of mixing attacks from professional hackers probably from the Russian Business Network[17] who used botnets and so called patriotic hackers– individual young users of computers who were outraged by Tallinn authorities decision to move the statue.[18] There was a special Russian language forum with the downloaded tools and instructions how to carry out cyberattacks[19].

Despite the initial surprise Estonia was able to organize defense quickly and with help of allies overcome the dangers. Germany, Israel, Slovenia and Finland provided assistance to restore normal networks operations. NATO Computer Emergency Response Team also helped Estonia.

Cyberattack on Estonia in 2007 was widespread reflected in media and called the first cyberwar in history. It showed how the new technology could be used to attack a modern country. The attack which came from Russia - most of the DDoS attacks were addressed from Russian IP addresses. A lot of attackers used computers from Estonia – it was the Russian minority. Even though, the European Commision and NATO technical experts did not find any evidence that this attack was perpetrated by Russian authorities, these attacks was very favorable to Kremlin.[20] It seems even more probable when the member of youth Russian organization NASI affiliated with the ruling party of Vladimir Putin confessed that he stood behind attacks.[21]

The presumable aims of the cyberattacks were to try to influence Tallinn authorities to withdrawn from its decision of removing the monument. Second was to test Russian cyber warfare capabilities and look for the reaction of NATO when one of the members of this organization is attacked in new domain. The third one was linked with the fact that Estonian society is dependent on the Internet. Cyberattacks were carried out to show that both NATO and EU would not defend Estonian society from the Russian attack and the Russian did not need tanks to inflict damages to Estonia. All political targets were not achieved, the monument was removed and Estonia became a leader on cybersecurity field. The NATO have sped up its cyberdefence projects and created Cooperative Cyber Defence Centre of Excellence located near Tallinn.

Georgia

Georgia regained its independence after the collapse of the Soviet Union. Unlikely as others post soviet republic this country had a long history and the strong national consciousness. From the beginning of 90s this country looked for integration with West.[22] This trend was strengthened after 2003 when the Rose Revolution[23] erupted and the current president Eduard Shevardnadze was overthrown. The new elected president Micheil Saakashvili engaged into integration with Western Structures and also tried to reintegrate the breakaways Georgian provinces – South Ossetia[24] and Abkhazia.[25] His attempts evoked a strong reaction from Russia which led to the war in 2008.[26]

This conflict which started on 7 August and lasted for 5 days was a remainder of classical states versus states wars which seems to be forgotten in the 21st century. Despite the fact, that the war was classical and the behaving of the armies on battlefield reminds the 20 century, one aspect of it was a complete novelty. It was the first war which took place in the air, on the ground, on the sea and in new domain – cyberspace.

The first cyberattacks took place months before the outbreak of war. On 19 July, the security firm informed about the Distributed Denial of Service (DDoS) attack against the Georgian websites. The similar scenario with the attacks on bigger scale was repeated on 8 August and coincided with the Russian troops entering the South Ossetia. The attack carried out by Russian hackers could be shared into two phases. In the first phase attacking hackers focused mainly on Georgian news and government websites. Russians used botnets to conduct mainly brute DDoS attacks. The Georgian networks were more vulnerable to attack than the Estonian ones.[27] In second phase of the cyberattacks the list of targets embraced financial institutions, businesses, educational institutions, Western media and a Georgian hackers website. Beside the DDoS attack there were also web defacement[28] operations done with using an SQL injection[29] and the massive spamming on public email in order to clog them. During the second phase of operation a lot of patriotic hackers joined campaign against Georgia[30]. Till 10 August the majority of the Georgian governmental Web sites were inoperative and Georgian Government was unable to communicate with the world using the Internet. Instead of normal content on the Georgian President website, there were images depicted M. Saakashvili as Hitler[31.] Also banks did not function in Georgia as well as the cell-phones[32]. Despite the fact that hacker were able to target Supervisory Control and Data

Acquisition (SCADA)[33] systems these kinds of attack were not observed. According to Captain Paulo Shakarian from the United States Army it means that Russian hackers tested their skills and ability to carry out limited attack. In future, in potential attacks against NATO countries attack on SCADA system could evoke the article V and the response could be more serious.[34]

The attacks came from the territory of Russia and were the mixture of professional acts carried out by using the botnets and the attacks conducted by patriotic hackers who similarly like in Estonia case could find information and programs on the special forums.[35] There was a list of prioritized targets and the information about potential vulnerabilities and how to evade Georgian blockade on Internet connections from Russia. The center of this information campaign was the website StopGeorgia.ru where the amateurs could find tools to carry out the DDoS attacks.[36] Similarly like in Estonia case experts did not find a clear direction between the Russian authorities and attack but the experts from Project Grey Goose - a voluntary organization consisted of 100 volunteers stated that "the level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government".[37] However, it seems that again Russian Business Network was engaged into attacks. Analysis of the different experts pointed out Alexandr A. Boykov a RBN operative and Andrey Smirnov a spammer from Saint Petersburg as two main perpetrators of cyberattack on Georgia. They represented vast knowledge and experience in carrying out hostile acts in cyberspace.[38]

There were two other interesting aspects of the cyberattack on Georgia. First one is the coordination of the conventional strikes and cyberattack which are mostly unseen. Nevertheless, there are two situations which could indicate the cooperation between classical and cyber forces. First one was the fact that conventional strikes omitted attacking the media and communication facility leaving these targets for cyberattacks. The second example was an attack on websites of renting diesel-powered electric generators in order to support conventional strike against Georgian electrical infrastructure.[39] The second interesting aspect is the preparation of the cyber tools, instruction, special websites to carry out the strikes. It can indicate that Russia was preparing this war for longer time. The access to tool available to Russians and the instructions how to use them could not be prepared in one day.[40]

The Georgian authorities in the wake of massive disruption of Internet websites firstly tried to filter Russian IP addresses but the Russian very quickly changed their tactic and used non-Russian servers.[41] Later Georgian authorities asked the allies the United States, Poland and Estonia for help. Georgians servers were relocated.[42]

The cyberattack on Georgia was a manifestation of information warfare aimed at cutting off Georgian authorities and society from any news. The perpetrators of it pursued to two main aims. First one was to demonstrate to the whole world the fragility of Saakashvili regime who lost control over the own state and Georgia in wake of Russian invasion had been paralyzed. Second one was addressed to Georgian society to cut them off from any information and present own propaganda in order to spread chaos and disinformation to undermine their morale and faith in government. Third target is linked with the second phase of attacks directed against the economic system. It was probably aimed to inflict serious damages for economic development of Georgia and persuade people to stop supporting Saakashvili. All aims were not achieved mainly because of the aid from allies. The government websites were restored and the Georgian society had an access to information and the United States promised financial help for Georgian government.[43]

Kyrygistan

The third country which suffered from massive cyberattacks was Kyrgyzstan. This republic located in the Central Asia was a part of the Soviet Union. After dissolution of it in 1991 Kyrygyzstan became a member of Commonwealth of Independence States. This

relatively small country with about 77 000 meteres square and 5 millions of people was a close ally of the Russia. This situation changed in 2005 when the Tulip Revolution overthrew long term President Askar Akayev. The new president was more pragmatic and tried to balance between the United States and Russia.[44]

The cyberattack took place in January 2009 when the heated debate rolled over the country about the future of American air force base in Manas. The strongest protests against closing the base came from the opposition. Manas base was established after the 11/09 when the United States prepared to attack Afghanistan. Kyrygystan supported George Walker Bush Administration in these efforts and agreed on the American Base on its own territory. In 2005 Kyrgyz President Kurmanbek Bakiyev during the meeting with Secretary of State Condoleezza Rice admitted that the American and NATO forces could use base till the situation in Afghanistan would be stable.[45] At the beginning of 2009 there was a discussion about the prolonging the renting of the base or closing it. This second option was supported by Russian government which proposed 300 million USD loan and 1.7 mld of investments in energy sector in order to influence Kyrygystan government to undertake the favorable decision.[46] In February 2009 Bakiyev announced that he would ask Americans to leave the base.[47] However, after the long negotiations the agreement between the Kyrygystan authorities and the United States were dealt in June 2009. According to the new agreement the cost for renting rose up from 16 million USD to 60 million USD and additionally, the United States promised additional investments.[48]

The attacks, which started on 18 January 2009 took place for 2 weeks. Attackers successfully disrupted 3 from 4 Internet providers service (IPS) included the two mains Kyrgyzstan IPS (www.domain.kg, www.ns.kg). They used massive DDoS attacks. Because there are only 4 IPS in in Kyrygystan, the majority of Internet services collapsed.[49] It was impossible to send email or enter to certain websties[50]and also using mobile phones was hindered because of cyberattack. Almost 80% of Internet traffic was offline. Nevertheless, the average citizens of Kyrygystan did not suffer because of the cyberattack from a simple reason. Only a small number of Kyrgyz had an Internet access.[51] However, it is important to stress that the opposition to the leading president was interdependent on the Internet.[52]

The IP traffic was traced backed to Russian servers where the most of DDoS traffic was generated[53]. These servers were commonly used to the cybercriminals activity as well as to attack Estonia and Georgia. The IP address and networks were associated with the groups responsible for previous attacks in 2007 and 2008. Also the two groups which led them were similar to these from 2008.[54] The high probability existed that behind these attacks stood the RBN. The probable scenario looked that Russian officials hired hackers from RBN to carry out the massive cyberattacks.[55]

The attacks were probably a part of Russian mounting pressure to persuade the Kyrgyz President Kurmanbek Bakiye to close American base in Manas. Especially, Russians wanted to silence the opposition which was against closing the base and tried to influence the president. Indeed, the Kyrgyzstan incident was the first case where these attacks successfully realized the political aim which had been to persuade Kyrgyz authorities to close the American base.

Conclusion

All attacks which took place between 2007 and 2009 had a lot of similarities: the political background is similar, the methods used by the aggressor are similar and also the hypothetical perpetrators are similar. There are also some differences like the main aims of attack and the result of it. However, these three cases set examples of mass cyberattacks aimed at paralyzing structures of the states.

Firstly, the political background just before the attacks is similar. All three countries in that time had tensed relationship with Russia. In case of Estonia in 2007 it was caused by

removal of the Bronze Soldier of Tallinn, in 2009 in Kyrygystan due to the heated debated about the future of Manas airbase. Ultimately, in case of Georgia it was a part of war but first time in a new domain – cyberspace. We clearly see that the cyberattacks carried out against these three former Soviet republics were done from political reasons.

The second interesting aspect is a technique of the attack. Here, we can notice similarities which can point out that the aggressor could be the same. However, the case of Georgia seems different and it was more sophisticated attack. The main tool of all attacks in all three cases were brute DDoS attack carried out firstly with using the massive botnet networks and later in case of Georgia and Estonia by patriotic hackers with using the earlier prepared tools. In case of Kyrygystan the patriotic hackers did not take part. The reason is that the attack on this Central Asia country was not so spectacular and did not gain the public support for this issue. The case of Georgia is slightly different. The attacks aimed at it were much more sophisticated and did not limit to the DDoS action mainly because it was a part of military campaign. It also embraced SQL injection attacks which could not be done by amateurs because it demands more advanced skills.

The third important point is the object of the attack. Here again we have a similar situation. In Georgia and Estonia the websites of government were disrupted, as well as the domains of banks and online newspapers. In case of Kyrgyzstan the attack was aimed at the providers on the Internet - which are only 4 in this country As the consequence of hostile action majority of the Internet services collapsed.

The fourth conclusion is linked with the vulnerability of the countries. It seems that the more dependent states from the Internet are more sensible on the attacks from cyberspace. Estonian citizens life was temporally hampered when the majority of Kyrgyzstan people did not spot that they were under the attack. It was caused that Estonia is highly dependent on cyberspace when Kyrgyzstan is not. On the other hand, the more advantageous countries like Estonia had more resilient networks and could easier restore their systems when they were under the attack. What is more, the disruption of the whole Internet is very difficult due to the big number of Internet providers.

The fifth point is the effectiveness of the action. In Estonia and Georgia cases the aggressors did not achieve their political aims. Both countries and their societies seemed to be resistant to the cyberattacks and did not revoke their policy after the cyberattacks. The different situation happened in Kyrgyzstan, where the cyberattacks combined with the political pressure influenced the decision to close the United States base. However, ultimately it changed and Americans could stay longer but for much more higher renting price.

One of the most important aspects of all three cases is the perpetrator of them. The architecture of cyberspace would not allow to unambiguously state who was responsible for cyberattacks. The fact is that the majority of the attacks came from Russia. We can conclude three hypotheses about it.

The first hypothesis is based on the assumption that attacks were carried out by the amateur, Russian, patriotic hackers who wanted to carry out the cyberstrike in order to express their outrage on the policy of Estonia and Georgia. This hypothesis is low probable mainly because of the lack of technical skills of these hackers. During the attacks the advanced botnets consisted of thousands of computers were used. There are inaccessible for average users of the Internet. What is more, in Kyrgystan case the Russian social networks of hackers were not involved in. The first hypothesis seems less reliable.[56]

The second hypothesis assumed that attacks were carried out by the Russian cybercriminal groups on their own, especially by the Russian Business Networks. Using the advanced botnets in all three cases owned by Russian cybercriminals pointed out the engagement of Russian hackers. These groups pursue mainly profits and money. It is hard to point out the potential financial benefits from attacking the Georgian, Estonian and Kirgiz websites and because of it these hypothesis also seems unreliable.[57]

The third hypothesis lies on the assumption that Russian authorities hired cybercriminals from Russian Business Network to carry out strike against Estonia, Georgia and Kyrgyzstan. This thesis seems the most probable because of the following reasons. Russia wanted to punish these countries but could not especially in case of Estonia - a NATO member - conduct the states sponsor offensive. So it was convenient to hire cybercrminals who carried the offensive campaign on behalf of Russian authorities.[58] The second important aspect is a full control for Internet flow in Russia by the Russian authorities and such a big attack could not be noticed by them.[59]

To sum up, the cases of Estonia, Georgia and Kyrgystan present a three similar scenarios of massive cyberattacks against states. The similarities between them point out that the perpetrator was the same. These actions prove that the cyberthreats could not be underestimated and in the future the similar actions will take place even with a bigger success.

References:

Internet Growth Statistics, retrieved from http://www.internetworldstats.com/emarketing.htm. (11.11.2013)

Arquilla John, Ronfeldt David, *Cyberwar is coming!*, [in:] Arquilla John, Ronfeldt David, ed. In Athena's Camp: Preparing for conflict in the information age, Washington: RAND Corporation, 1993.

More about the history of Estonia you can find: *Estonia's history. Chronology*, retrieved from http://estonia.eu/about-estonia/history/estonias-history.html (11.11.2013).

Population by Nationality, retrieved from http://estonia.eu/about-estonia/country/population-by-nationality.html (11.11.2013).

Szakonyi David, *The Rise of Nationalism under Globalization and the Case of Post-Communist Russia*, retrieved from http://www.sras.org/economic_nationalism_under_globalization (11.11.2013).

Terlikowski Marcin, *Cyber attacks on Estonia. Implications for international Polish Security*, "Polish Quarterly of International Affair", 2007 p.75.

Tallinn tense after deadly riots, 28 April 2007, retrieved from http://news.bbc.co.uk/2/hi/6602171.stm (11.11.2013.).

Myers Lee Steven, *Friction Between Estonia and Russia Ignites Protests in Moscow*, retrieved from http://www.nytimes.com/2007/05/03/world/europe/03estonia.html (11.11.2013.)

Kaeo Merike, *Cyber attacks on Estonia. Shot Synopsis*, retrieved from http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf (11.11.2013).

Botnet are networks consisted of infected computers which are used to carry out cyberattacks. The users of these infected computers called zombies computers are unaware that they participate in attack, *What is a botnet?*, retrieved from http://www.microsoft.com/security/resources/botnet-whatis.aspx (11.11.2013).

Kaeo Merike, op. cit.

Distributed Denial of Service is an attack on computer service in order to disrupt it. It is based on flooding with too many connections request. We can enumerate two kinds of DDoS attack brute and semantic attacks Brute DDoS attacks appeared when the target receives more Internet traffic than it can handle. Semantic attacks are more sophisticated. Mirkowic Jelena, Reiher Peter, *A Taxonomy of DDoS Attack and DDoS Defence Mechanisms*, ACM SIGCOMM Computer Communication Review 34, No. 2, April 2004, p. 39 – 53.

Ruus Kertu, *Cyber War I: Estonia Attacked from Russia*, http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/cyber-war-i-estonia-attacked-from-russia.html (11.11.2013).

Terlikowski Marcin, *op. cit*., p. 75.

Ruus Kertu, op. cit.

More about the main DDoS attack in history you can find: *DDoS Attack Timeline , retrieved from The History & Changing Nature of DDoS Attacks*, retrieved from http://www.defense.net/index.php/ddos-in-depth/ddos-timeline/ (11.11.2013).

Russian Business Network is the biggest and most famous cybercriminal group. It offers a variety spectrum of tools and methods. . According to the IT security experts this organization possessed the largest botnets with between 150 and 180 millions of infected computers. More on this topic you can find: Matyska Piotr, *RUSSIAN BUSINESS NETWORK - próba ustalenia faktów*, retrieved from http://www.psz.pl/RUSSIAN-BUSINESS-NETWORK-proba-ustalenia-faktow (12.11.2013).

Kaeo Merike, op. cit.

Herzog Stephen, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, "Journal of Strategic Security, Vol. 4, No. 2, 2011, p. 51.

Estonia has no evidence of Kremlin involvement in cyber attacks, 06/09/2007, retrieved from http://en.ria.ru/world/20070906/76959190.html (11.11.2013).

Shachtman Noah, *Kremlin Kids: We Launched the Estonian Cyber War*, 03.11.09 http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/ (11.11.2013).

More about Georgia in 90s you can find in: Cornell E. Svante, *Small Nations and Great Powers: A Study of Ethnopolitical Conflict*, Ney York: Routledge 2001.

More about the Rose Revolution you can find in: King Charles, *A Rose Among Thorns. Georgia Makes Good*, "Foreign Affairs", Vol. 83, No.2, March/April 2004, p. 13 – 18.

More on South Ossetia you can find in: *Regions and territories: South Ossetia*, 25.04.2012, retrieved from http://news.bbc.co.uk/2/hi/africa/country_profiles/3797729.stm (11.11.2013).

More on Abkhazia you can find in: Hewitt George, *Abkhazia, Georgia, and history: a response*, 25.08.2009, retrieved from http://www.opendemocracy.net/article/abkhazia-georgia-and-history-a-response (11.11.2013).

More about war in Georgia you can find in: Asmus Ronald, *Little War that Changed the World. Georgia, Russia and the Future of the West*, New York: Palgrave Macmillan, 2010.

Shakarian Paulo, *The 2008 Russian Cyber Campaign Against Georgia*, Military Review, November-December 2011, p. 63-64.

Website Defacement is an unauthorized changed done on the website against the will of owner of it. Sometime websites are replaced completely. *What Is Website Defacement?*, 05.03.2013, retrieved from http://www.websitepulse.com/blog/what-is-website-defacement (11.11.2013).

SQL injection uses a text field on webpage to directly communicate with the back end database. The successfully using SQL injection gives the hacker total access to the database. Ullricha B. Johannes, Lamb Jason, *Defacing websities via SQL injection*, Network Security, January 2008, p. 9-10

Shakarian Paulo, op. cit. p. 64.

Korns W. Stephen, Kastenberg E. Joshua, *Georgia's Cyber Left Hook*, "Parameters", p. 60

Corbin Kenneth, *Lessons From the Russia-Georgia Cyberwar*, 12.03.2009, retrieved from http://www.internetnews.com/government/article.php/3810011 (11.18.2013).

SCADA systems are based on collection, control and monitor of critical infrastructure (power plants, oil and gas pipelines, refineries and water systems) Fernandez D. John, Fernandez E. Andres, *SCADA systems: vulnerabilities and remediation*, "Journal of Computing Sciences in Colleges" Vol. 20, No. 4 April 2005, p. 160-168.

Shakarian Paulo, op. cit, p. 66.

Korns W. Stephen, Kastenberg E. Joshua, op. cit., p. 65.

Morozov Evgeny, *Army of Ones and Zeros: How I became a soldier in the Georgia-Russia Cyberwar*, 14.07.2008, retrieved from http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html (18.11.2013).

Krebs Brian, *Report: Russian Hacker Forums Fueled Georgia Cyber Attacks*, 16.10.2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html (17.11.2013).
RBN - Russian Cyberwar on Georgia: Report, retrieved from http://rbnexploit.blogspot.com/2008/10/rbn-russian-cyberwar-on-georgia.html (11.11.2013).
Shakarian Paulo, op. cit., p. 66.
Ibidem.
Shakarian Paulo, op. cit., p. 65.
Korns W. Stephen, Kastenberg E. Joshua, op. cit., p. 60.
Georgia: One year after the August war. Testimony of Ambassador Alexander Vershbow, Assistant Secretary of Defense for International Security Affairs, 4 sierpnia 2009 r., retrieved from http://reliefweb.int/node/319521 (11.11.2013).
Górecki Wojciech, *Rosja wobec wydarzeń w Kirgistanie* (April-June 2010), retrieved from http://www.osw.waw.pl/pl/publikacje/komentarze-osw/2010-07-27/rosja-wobec-wydarzen-w-kirgistanie-kwiecien-czerwiec-2010 (11.11.2013).
Kyrgyzstan Under DDoS Attack From Russia, ?The Cyber Attack No One Is Talking About?, retrieved from http://www.secureworks.com/resources/blog/research/research-20957/ (11.11.2013).
Russia-presses-kyrgyzstan-to-close-us-base, retrieved from http://www.smh.com.au/news/world/russia-presses-kyrgyzstan-to-close-us-base/2009/01/18/1232213448844.html (11.11.2013).
Kyrgyzstan to shut key NATO base, 04.02.2009, retrieved from http://rt.com/usa/kyrgyzstan-to-shut-key-nato-base/ (11.11.2013).
Nichol Jim, *Kyrgyzstan and the Status of the U.S. Manas Airbase: Context and Implications*, July 1, 2009, Congressional Research Service7-5700, p.1, retrieved from http://www.fas.org/sgp/crs/row/R40564.pdf (11.11.2013).
Kyrgyzstan Under DDoS Attack From Russia? The Cyber Attack No One Is Talking About,, retrieved from http://www.secureworks.com/resources/blog/research/research-20957/ (11.11.2013).
Mackey Robert, Are 'Cyber-Militias' Attacking Kyrgyzstan?, 5.02.2009, retrieved from http://thelede.blogs.nytimes.com/2009/02/05/are-cyber-militias-attacking-kyrgyzstan/?_r=0 (11.11.2013).
Bradbury Danny, *The fog of cyberwar*, retrieved from http://www.theguardian.com/technology/2009/feb/05/kyrgyzstan-cyberattack-internet-access (11.11.2013).
Keizer Gregg, *Russian 'cybermilitia' knocks Kyrgyzstan offline*, 28.01.2009, retrieved from http://www.computerworld.com/s/article/9126947/Russian_cybermilitia_knocks_Kyrgyzstan_offline (11.11.2013).
Carroll Ward, *Russia Now 3 and 0 in Cyber Warfare*, January 30, 2009. retrieved from http://defensetech.org/2009/01/30/russia-now-3-and-0-in-cyber-warfare/#ixzz2kC8saBkH (11.11.2013).
Keizer Gregg, op. cit.
Carroll Ward, op. cit.
Shakarian Paulo, op. cit., p.66.
Ibidem, p. 67.
Ibidem, p. 67.