PRZEGLĄD ZACHODNI
2013, No. II

MIRON LAKOMY
Katowice

# CYBER THREATS AT THE BEGINNING OF THE 21ST CENTURY

The very concept of cyberspace was popularised by *Neuromancer*, a science fiction novel by William Gibson. His *cyberspace* referred to a world of digital networks where interests of huge corporations clashed. Along with advancements and dissemination of information technologies, the word was adopted by academics. Cyberspace is a new dimension of human activity which Pierre Lévy defined as the new medium of communications that arouse through the global interconnection of computers. It is an open space where human beings communicate, and a network of IT memories. Another definition offered by Marie Laure Ryan emphasises that cyberspace is a virtual reality generated by machines.[1] Initially, IT networks were primarily used by research and military institutions. With the launch of the PC and the Internet, the importance of cyberspace started to grow rapidly. The process of computerisation and digitalisation began to include increasingly more areas of states' and societies' operations and activities. Regardless of enormous advantages of the above, the processes initiated were to bring about serious threats. Originally, they were single attacks by individuals for whom hacking was a hobby. Over time, however, the nature of that activity has changed. At the turn of the 21st century, hackers began to organise themselves in independent groups increasingly supported by state governments. The once petty cases of breaking into computer systems gradually evolved to orchestrated actions of groups of programmers collaborating with secret services, the aim of which was to obtain a specific political, economic or military advantage. Moreover, on-line attacks did not focus on websites only; increasingly often, they targeted servers and networks of critical importance to the functioning of state structures. Thus, at the beginning of the 21st century, cyberspace became an arena of activities that threaten not only the security of classified information but also the functioning of critical infrastructure.[2] Therefore, it is worth to consider measures taken by states and international organisations to adapt to the new security situation at the turn of the first and second decade of the 21st century.

---

[1] M. Lakomy (2010), *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, "Stosunki Międzynarodowe" No. 3-4, p. 56.

[2] *Ibid.*, p. 56.

## NEW CHALLENGES FOR NATIONAL CYBERSECURITY AT THE TURN OF THE 21ST CENTURY

Activities of both states and non-state groups in cyberspace can generally be divided into three groups: cyber terrorism, cyber espionage, and the use of cyberspace for military purposes.

Cyber terrorism is usually defined as an attack on computers, networks and/or information systems, aimed at achieving a specific political advantage. Already in the 1980s, both the United States and the Soviet Union made first attempts to use cyberspace to that end. However, the attempts were sporadic cases of relatively minor importance. In the 1990s, the situation changed somewhat due to the Internet popularisation and digitalisation of increasingly more areas of life. First threats were generally caused by hobbyists who developed computer viruses. In the second half of the 1990s, the number of hacking attacks on computer networks and government institutions grew. Hacking attacks were performed not only by individual hackers, but organised crime groups as well. In the first decade of the 21st century, cyberspace began to be exploited by states. Groups of hackers hired by governments to accomplish certain tasks in the Internet began to play a special role.

The turning point in the debate on cyber threats were undoubtedly events in Estonia in April 2007. Then, a heated political debate between Tallinn and Moscow on the removal of a Soviet war memorial led to a massive attack on the Estonian Internet. Groups of Russian hackers, who used the so called botnet[3], paralysed not only most important public and private institutions, but also, inter alia, the banking system. The scale of their attack was unprecedented. Though, according to experts, the on-line attack on Estonia resembled more "cyber riots" than a "cyber war", it proved the growing importance of information and communication networks for the state security.[4]

The growing importance of cyber terrorism in state politics was further confirmed during the Russia-Georgia War in 2008. During that armed conflict, for the first time the potential of cyberspace was exploited in addition to traditional instruments of warfare. Like in the case of Estonia, throughout almost the entire period of the conflict, Russian hackers associated in the *Russian Business Network* were able not only to block websites of the Georgian government, academic institutions and major mass media, but also communication infrastructure, e.g. mobile VoIP. On the official website of President of Georgia Mikhail Saakashvili, they posted materials accusing Tbilisi of starting the war. The photo of the president was replaced with

---

[3] Botnet is a group of PCs infected with malware and covertly controlled by a group of hackers. B. Łącki, *Botnet od podszewki (Botnet inside out)* Heise Security,13.06.2007. http://www.heise-online.pl/security (accessed 25.01.2011).

[4] S. Waterman, *Who Cyber Smacked Estonia,* 11.06.2007, http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/ (accessed 25.01.2011).

a photo of Adolf Hitler, which had a strong propaganda effect. During the war, Russians proved their very high potential in cyberspace operations which enabled them to effectively block the Georgian government's efforts to inform the world about events in South Ossetia. The Georgian Minister for Foreign Affairs was forced to use a Google blog. President Saakashvili also faced similar problems not being able to contact journalists wanting to interview him by phone. The events in the Caucasus in August 2008 have been called the "second cyber war", during which the ICT space was massively used against another country. According to Kevin Coleman, an expert in cybersecurity, the above proved that this new aspect of state security could not have been ignored any longer. Cyberspace has become an integral part of modern armed conflicts. Bill Woodcock shares Coleman's view, emphasising that cyber attacks are extremely dangerous, cheap and easy to mount, and will remain a feature of modern warfare.[5] Interestingly, the third "cyber war" started only a few months later. In early 2009, there were massive cyber terrorist attacks in Kyrgyzstan. The reason for blocking almost the entire Kyrgyz Internet, again by Russian hackers, was a discussion held in that country on the US future access to a military base.[6]

The emergence of new cyber terrorist threats was also confirmed by the events in Iran. As experts point out, Israel has developed the most advanced computer virus ever, designed specifically to paralyse Iran's nuclear power plants. The worm, called Stuxnet, was introduced to computer systems in plants in Natanz and Bushehr by Russian subcontractors. Due to its highly complex design, the worm successfully interrupted the operation of uranium enrichment centrifuges which, in some opinions, effectively slowed down the Iranian nuclear programme. The exceptionality of the Stuxnet worm consists in its highly specialized malware payload. It has been designed solely to attack computer systems that control industrial processes in nuclear power plants and tinkers feedback software concealing its existence.[7] It needs to be added that increasingly often cyberspace is used by terrorist organisations. For example, at the beginning of the 21st century, possibilities of computer attacks for the purpose of propaganda, training, and recruitment were examined by Al-Qaeda and Hezbollah.[8]

---

[5] J. Markoff, *Before the Gunfire, Cyberattacks, "*The New York Times" 12.08.2008; K. Coleman, *Cyber War 2.0 -Russia v. Georgia,* DefenseTech, 13.08.2008. http://defen-setech.org (accessed 12.03.2011); M. Lakomy (2010), *Znaczenie cyberprzestrzeni...,* p. 61.

[6] K. Coleman, *Russia Now 3 and 0 in Cyber Warfare,* DefenseTech, 30.01.2009. http://defensetech.org (accessed 12.03.2011).

[7] A. Aneja, *Under cyber-attack, Iran says, "*The Hindu" 26.09.2010; *Stuxnet heralds age of cyberweapons, virtual arms race, "*Homeland Security Newswire" 27.01.2011, http://homeland-securitynewswire.com (accessed 01.03.2011); *To był izraelski cyber-atak na Iran*, Dziennik.pl, 01.10.2010, http://wiadomosci.dziennik.pl (acccessed 01.03.2011).

[8] S. Moćkun (2009), *Terroryzm cybernetyczny - zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, Raport Biura Bezpieczeństwa Narodowego, Warsaw, July, p. 2; M. Łapczyński (2009), *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, "Pułaski Policy Papers" No. 7, p. 1; P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, in: L. H. Haber (ed.) (2003), *Społeczeństwo informacyjne - wizja czy rzeczywistość?*, Kraków, pp. 376-377.

Cyber espionage can be defined as an attempt to steal classified information from servers or networks of both public and private institutions. The People's Republic of China plays a special role here, since it was the first country to use computer hacking on a large scale to obtain new technologies and secret information. Already in 2003-2005, Chinese hackers carried the *Titan Rain* operation which consisted in a series of attacks on servers of research and military institutions in the United States. Hackers stole the project data on the next generation *F-35 Joint Strike Fighter*. In another series of cyber attacks carried in the late 1990s and known as the *Moonlight Blaze*, Russian hackers targeted a number of servers of American research and military institutions, stealing, inter alia, information about the American missile system.[9]

In 2008, the most serious hacking attack ever targeted US military networks. Probably Russia was involved. No information was disclosed about the volume of secret information lost, but the incident must have had serious consequences as it took American programmers 14 months to remove the malware.[10] Around the same time, another serious attack was carried out by a group of Chinese hackers called *GhostNet*. They broke into nearly 1,300 computers of governmental institutions, corporations and research institutions in 103 countries. Considering its geographical range, it has been the largest spy attack carried out via the Internet.[11] Further increase in China's activities was proved by the *Aurora* operation carried out in the second half of 2009. Chinese programmers attacked servers of about 20 US corporations, including Google, Yahoo and Symantec, to gain access to new technologies.[12]

Last but not least, there is the possibility of using cyberspace in armed conflict conditions. In the mid-1990s, J. A. Warden recognised communication networks to be the fifth component of armed combat.[13] Already during the war in Kosovo, there were cyber incidents but they were of practically no significance. It was in Georgia, in 2008, where massive cyber attacks were carried out in armed conflict conditions. The attacks by Russian hackers, however, had political and propaganda purposes mainly. That is why, they are usually classified as instances of cyber terrorism.

The enormous potential of using cyberspace while conducting military operations was demonstrated by Israel in September 2007. The IDF Air Force carried out the operation *Orchard*, the aim of which was to destroy a Syrian nuclear facility of a military purpose. The airstrike was successful as IDF aircrafts were not detected by the Syrian anti-aircraft defence system. This was possible because the Syrian air defence network was compromised by a computer virus introduced by the Israelis. It

---

[9] M. Łapczyński (2009), *Zagrożenie cyberterroryzmem...,* p. 1; P. Sienkiewicz, *Wizje i modele...,* pp. 376-377.

[10] W. J. Lynn III, *Defending a New Domain,* "Foreign Affairs" September/October 2010.

[11] S. Adair, R. Deibert, G. Walton, *Shadows in the Cloud: Investigating Cyber Espionage 2.0,* "Information Warfare Monitor" Shadowserver Foundation, 06.04.2010.

[12] K. Jackson Higgins, *'Aurora' Attacks Still Under Way, Investigators Closing in on Malware Creators, "*Dark reading" 10.02.2010, http://www.darkreading.com (accessed 10.03.2011).

[13] J.A. Warden (1995), *Enemy as a System,* "Airpower Journal" No. 9, pp. 40-55.

enabled the IDF to control Syrian radars, so that IDF aircrafts remained undetected while flying over Syria. That event clearly proved that cyberspace could be successfully used in an armed conflict. It was the use of the telecommunication space which made it possible, i.e. to achieve a result that would be almost impossible with traditional methods.[14]

To recapitulate, in the first decade of the 21st century, cyber threats to the security of states started snowballing. They are not only incidental events caused by a single person or small groups of programmers, but increasingly often they are massive, organised attacks motivated and/or carried out by national governments to achieve some political, military or economic advantage.

## PERCEPTIONS OF CYBER THREATS IN SECURITY POLICIES OF SELECTED INTERNATIONAL ACTORS

Focusing on the threats discussed above, it is worth to consider how, in the early 21st century, the issue of cybersecurity has been addressed by most prominent actors in the international arena. Certainly, the leader in the fight against cyber threats is the United States which, currently, experiences the largest number of hacker attacks in the world. In 2008, the servers of the Department of State were attacked nearly six million times per day, which clearly illustrates the scale of the problem.[15] As it was mentioned earlier, US intelligence service made their first steps in cyberspace in the 1980s, but they had a symbolic meaning only and did not meet with the interest of policy makers. The scale of cyber threats, however, was recognised in the US relatively early, i.e. in January 1995. The US Department of Defense established the *Information Warfare Executive Board* responsible for protecting US interests in the ICT environment. Moreover, it was also in the US where the research on the effects of the use of cyberspace in a traditional armed conflict began. The turning point for the US cyber security policy was certainly the presidency of George W. Bush, whose administration published *The National Strategy to Secure Cyberspace* in February 2003. In the document it was recognised that securing cyberspace was a strategic challenge for the United States. The document also read: "Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security". The American strategy had 5 priorities:

– development of a *National Cyberspace Security Response System*, including both state and private entities;

---

[14] D.A. Fulgham, *Why Syria's Air Defense Failed to Detect Israelis,* "Aviation Week and Space Technology" 03.10.2007.

[15] M. Łapczyński (2009), *Zagrożenie cyberterroryzmem...,* p. 1; P. Brągoszewski (2007), *Świat żywych trupów,* "PC World" May.

- introduction of a National Cyberspace Security Threat and Vulnerability Reduction Program based on the cooperation of particular state agencies and a system of analysing the regularity of attacks in ICT networks,
- promotion of a national Cyberspace Security Awareness and Training Program, aimed at making Americans aware of Internet threats;
- introduction of new technological solutions securing government cyberspace;
- fostering cooperation in the field of cyber security not only between different government agencies but also with other countries in the so-called Safe Cyber Zone.[16]

The true turning point in American cyberspace security policy and in other countries' policies, however, was the "first cyber war" in Estonia. In January 2008, experts began to develop the Comprehensive National Cybersecurity Initiative which was to be a coherent response of the US government to Internet threats. The CNCI consisted of 12 separate projects, addressing, inter alia, deployment of intrusion detecting systems identifying unauthorized users' attempt to gain access to government networks, development of R&D projects on cybersecurity and coordination of research in this area. An extensive report prepared for Barack Obama by the Center for Strategic and International Studies (CSIS) December 2008 should also be mentioned. The document reads that cyber threats are major challenges to the state security in the 21st century. In its authors' opinion, a new strategy is needed that would include not only traditional political, economic, and military components, but cybersecurity issues too. In their view, the fight against cyber threats should be multidirectional. Firstly, due to the nature of the threats, government agencies should cooperate with the private sector. Secondly, the government should establish minimum security standards for telecommunication networks to ensure that core services in cyberspace will continue to be provided. Thirdly, the US should develop technologies which will identify web users better. Fourthly, the US legislation should be updated since the existing provisions have not efficiently provided for cybercrime cases. Fifthly, the US administration should purchase necessary ICT technologies. Last but not least, the US should conduct research and educational programmes strengthening the US leadership in cyberspace.[17]

President Barack Obama has largely followed the above mentioned recommendations and cybersecurity has become a priority for the new administration. One of first decisions taken by Obama was to appoint the US Cybersecurity Coordinator and create the Cybersecurity Office within the National Security Staff. The work of the new entity resulted in a report titled "Cyberspace Policy Review", which defines key objectives of US cyber security policy including establishment of structures needed to combat cybercrime, appointment of an official to ensure privacy and civil liberties

---

[16] M. Lakomy (2010), *Znaczenie cyberprzestrzeni*..., pp. 61-64.

[17] *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic and International Studies, December 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf .

in cyberspace, initiatives raising public awareness about on-line threats and development of crisis response plans to counter attacks in American cyberspace.[18]

A direct outcome of the conceptual work, which began in 2008, was that new entities and structures were established to protect American cyberspace. The Department of Homeland Security and the National Security Agency have established a unit composed of ca. 2000 computer experts whose task is to conduct both defensive and offensive operations in cyberspace. Moreover, the National Cyber Security Division was established which is part of the Department of Homeland Security. Its task is to monitor, analyse, and protect the American Internet. The most important decision, however, was the creation of the United States Cyber Command in June 2009. Its tasks include, inter alia, coordination of the US defence network in cyberspace and carrying out attacks. The command consists of e.g. the 10th Fleet and the Marine Corps Forces Cyberspace Command. [19] An interesting result of the conceptual work on cybersecurity was a provision that in the case of an attack on network servers crucial to the state interest, the US administration may cut off some telecommunication networks.[20] Despite the above efforts, according to Mike McDonnell, a former US National Intelligence Director, the US still does not have the capacity sufficient to defend itself against most serious attacks on, for example, its critical infrastructure components.[21]

Not long ago, cyberspace threats have been recognised also by decision-makers in Poland. Like in other countries, the turning point were the events in Estonia and Georgia, which demonstrated that the risk of a conflict outbreak in cyberspace is high. First references to cybersecurity were made in the 2007 *National Security Strategy of the Republic of Poland* but they were fairly general. Taking into account the experience of Estonia and Georgia, and the systematically increasing number of attacks in the Polish Internet, in 2008 the Internal Security Agency took steps to review the security status of servers and websites of government institutions. The next step was the *Governmental Programme for the Protection of Cyberspace in Poland for the Years 2009-2011* approved on 9 March 2009. Its introduction reads that cyber terrorism has now become a key and growing form of terrorist attacks. The general objective of the programme was to raise the level of the state's cyberspace security. Specific objectives included e.g. improvement of Poland's critical ICT infrastructure security, development and implementation of a single cyberspace security policy for all state institutions, reduction of a cyber attack impact, development of a sustainable coordination system covering the private sector and government institutions, widening of cybersecurity competences of entities involved in the protection of the state

---

[18] M. Lakomy (2010)*, Znaczenie cyberprzestrzeni...*, pp. 64-65.

[19] *Memorandum for Secretaries of the Military Departments*, The Secretary of Defense, Washington D.C., 23.05.2009.

[20] T. Romm, *NCTA praises Rockefeller-Snowe cybersecurity bill*, "The Hill" 18.03.2010.

[21] M. Bosacki, *Cyberwojna: Chiny vs USA*, "Gazeta Wyborcza" 02.02.2010.

infrastructure, and raising the awareness of users of ICT networks in that regard.[22] The document was, in fact, the very first national strategy which comprehensively addressed the cybersecurity issue.

In June 2010, experts of the Ministry of Defence, Internal Security Agency, Border Guard, and the Research and Academic Computer Network NASK completed their work on a document covering the government's plans for the next six years. *The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016* has been much improved in comparison to the previous programme. In the preface, the authors wrote: " In the face of globalization, the cyberspace security has become one of the key strategic objectives in the area of security of each country." According to the authors, in the 21st century, the thin line between peace and war becomes increasingly more conventional. In consequence, there is an increasing need for cooperation between public (military) and private (civilian) sectors. Provisions of the new programme cover not only ITC systems and networks belonging to state institutions but also those of companies of strategic importance to the state, and natural persons using the cyberspace. Interestingly, the document does not cover classified ICT networks and systems, the protection of which is regulated by separate provisions. Unlike in the earlier version, key terms were defined:

- cyberspace - a space of processing and exchanging information created by the ICT systems;
- cyber terrorism – an offence of a terrorist nature committed in cyberspace;
- cyber attack – an intentional disruption of the proper functioning of cyberspace;
- incident - a single event or a series of adverse events related to information security;
- critical ICT infrastructure – critical infrastructure distinguished within communication and ICT systems.

The strategic objective of the document is to achieve an acceptable level of cyberspace security of the state. Specific objectives include:

- increasing the level of security of the state ICT infrastructure;
- improving the capacity to prevent and combat threats from cyberspace;
- reducing the impact of incidents threatening the ICT security;
- determining the competence of entities responsible for the security of cyberspace;
- creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors;
- creating a sustainable system of coordination and exchange of information between the entities responsible for the security of cyberspace and the cyberspace users.

---

[22] *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011(Governmental Programme for the Protection of Cyberspace in Poland for 2009-2011*), CERT, Warsaw, March 2009, www.cert.gov.pl (accessed 02.02.2011).

– increasing awareness of the cyberspace users of the methods and safety measures in cyberspace.

The programme implementation is the responsibility of the Ministry of the Interior (and Administration), Ministry of Defence, National Security Agency, and the Military Counterintelligence Service. Major objectives of the programme include:

– making relevant state authorities obliged to report the risks and problems encountered in cyberspace to the Ministry of the Interior;
– taking legislative measures to adapt present legislation to tasks set out in the programme;
– reorganising the existing national cyberspace infrastructure to its full potential;
– education of current and future ICT users;
– technological advances aimed at reducing cyber threats;
– identification of entities responsible for the protection of Poland's cyberspace;
– legal recognition of the Governmental Computer Security Incident Response Team (CERT);
– appointment of the Intra-Government Coordination Team for the Protection of Poland's Cyberspace;
– appointment of plenipotentiaries for the protection of cyberspace in organisational units of government administration;
– introduction of ICT security topics as a permanent element of higher education to ensure a supply of qualified personnel;
– providing training to civil servants;
– conducting social campaigns aimed to raise awareness of the risks appearing in cyberspace;
– undertaking national research programmes on cyber security issues;
– expansion of cyberspace incident response teams, early warning emergency systems, and on-going testing of security measures;
– development of Computer Security Incident Response Teams (CERT) in government administration;
– preparation of Continuous Action Plans.[23]

The document has as many as 26 attachments addressing, inter alia, the development of CERTs and the Internal Security Agency's cooperation with NATO. This programme has been thus significantly improved as compared to the 2009-2011version. It seems that it constitutes a proper response to the most serious challenges for Poland's ICT security.

The most significant outcome of the government's interest in cyber security issues was the decision of 1 February 2008 to appoint the Government Computer

[23] Cf. *Rządowy Program Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016,* Ministry of Interior and Administration of the Republic of Poland, Version 1.1., Warsaw, June 2010, and *Cyberspace Protection Policy of the Republic of Poland*, Ministry of Administration and Digitisation, Internal Security Agency, Warsaw, 25 June 2013, https://mac.gov.pl/wp-content/uploads/2013/06/Polityka-Ochrony-Cyberprzestrzeni-RP_wersja-ang.pdf

Security Incident Response Team (CERT), established under the agreement between the Ministry of Interior (and Administration) and the Internal Security Agency. The CERT tasks include: coordination of the incident response process, publishing announcements concerning security threats, resolving and analysing incidents (including collection of evidence by a team of forensics), publishing notifications (security bulletins), coordination of responses to security weak spots, detection of incidents in networks protected by the ARAKIS-GOV system and administering security tests. It should be noted here that responsibilities of the CERT covers only government servers and the state critical infrastructure.[24] In August 2009, plans to establish the first Polish military unit designed to operate in cyberspace and protect the Ministry of Defence and military commands against cyber attacks, were disclosed. In mid-2010, the Cyber Security Centre was established as part of the 9th Signal Battalion in Białobrzegi, the operation of which is strictly confidential. In 2010, there was also some information that the Ministry of Defence foresees establishment of the first "digital" battalion of the Polish army.[25] The government also plans to appoint a plenipotentiary for cyberspace security, whose main task will be to coordinate the work of all departments involved in the protection of ICT networks.[26] The signing of the Poland-US agreement on the exchange of information and network security on 21 June 2010, was another important event demonstrating Poland's growing interest in cyberspace. Director General of the Ministry of National Defence Jacek Olbrycht commented on the event as follows: "I am deeply convinced that the agreement will allow both parties to increase the capabilities of prevention, detection, and reaction to cyber attacks, as well as ensure appropriate protection of information being processed in information and communication systems.".[27]

NATO has also recognised the importance of cyberspace, which was primarily due to the events in Estonia in 2007. NATO's first response to the Estonian crisis was to send a group of its best experts on cybersecurity to Tallinn. At the time it was questionable as allies' obligations under Article 5 of the North Atlantic Treaty of 1949 do not cover cyberspace. Only after those events, NATO Secretary-General Jaap de Hoop Scheffer declared that the Alliance would include cyber security issues into its new strategy. The Estonian crisis met with a concrete response in 2008 when the decision to establish a new NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) in Tallinn was taken. Its mission is to conduct research on cyber warfare. The following countries have participated in the work of the Estonian CoE:

---

[24] M. Lakomy (2010), *Znaczenie cyberprzestrzeni...,* pp. 64-65.

[25] *Wojsko polskie tworzy cyfrowy batalion,* Polskie Radio, 01.12.20101, http://www.polskieradio.pl (accessed 02.02.2011); *Armia ma sposoby na ataki hakerów,* Newsweek.pl, 01.12.2010, http://www.newsweek.pl (acccessed 02.02.2011).

[26] S. Czubkowska, *Polska cyberprzestrzeń będzie pod specjalnym nadzorem,* Forsal.pl, 14.09.2010, http://forsal.pl (accessed 10.02.2011).

[27] *Polish-US MoU on information exchange and network security*, Ministerswtwo Obrony Narodowej, 21.06.2010.

United States of America, Slovakia, Italy, Spain, and the Baltic States.[28] Cyber security issues were fully regulated in the new NATO's *Strategic Concept*, adopted at the Lisbon Summit in November 2010. It provided for the fact that cyberspace terrorism is a major threat to the security of NATO member states in the 21st century. As cyber attacks become increasingly more frequent, more organised and harmful to government administrations, businesses, economies and potentially also to transportation and supply networks and other critical infrastructure, they may reach a threshold beyond which they will threaten both national and Euro-Atlantic stability and security. That is why, the Heads of State and Government of the NATO member states have declared that NATO needs to develop instruments that will allow it to respond to any kind of threat. It has been decided that NATO will develop its capacities to prevent, detect and defend against cyber attacks, inter alia, by coordinating activities of government agencies and bringing all NATO bodies under centralised cyber protection.[29] As of today, NATO's cyber defence policy is based on four pillars:

- coordination and advising on cyber defence which has included the establishment of the Cyber Defence Management Authority (CDMA), headed by the Cyber Defence Management Board, consisting of the heads of the agencies of member states involved in ensuring cybersecurity. The main task of this institution is to coordinate activities of member states in area of NATO ICT data networks' protection;
- research and training: they take place at the CCD CoE established in Tallinn, which is part of NATO's new Emerging Security Challenges Division. It consists of ca. 30 professionals;
- assistance to member states: the Alliance has been developing mechanisms to provide immediate assistance to the states that fell victim of attacks in cyberspace using Rapid Reinforcement Teams (RRT), i.e. groups of experts in cyber defence. The support provided to Estonia in 2007 was a manifestation of this policy;
- cooperation with other international partners and organisations: exchange of experience and information, and - in some cases - mutual assistance.[30]

The importance of this dimension of security for the Alliance was confirmed by consultations between US Deputy Secretary of Defense William J. Lynn and representatives of NATO and its member states held in January 2011 in Brussels. During the talks, the importance of cooperation between government agencies and private sector entities was strongly underlined.[31]

---

[28] C. C. Chivvis (2009), *Considerations on NATO's Future Direction,* "Politique étrangère" No. 4, p. 65.

[29] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation,* Adopted by Heads of State and Government, NATO, Lisbon, 19.11.2010.

[30] *NATO's cyber defence policy and activities,* North Atlantic Treaty Organisation, http://www.nato.int (accessed 04.02.2011).

[31] J. Garamone, *Lynn Discusses Cybersecurity with NATO, U.S. leaders,* U.S. Department of State, American Forces Press Service, 24.01.2011.

Until 2010, the European Union showed little interest in solutions in this area. In 2010, it intensified its work on a strategy to prevent cyber threats. The European Commission plays a special role in that respect since it is working on a package of legislation governing this security dimension. One of the European Commission's proposals is to, inter alia, provide for a full penalisation of all hacking software used in cyber attacks.[32] The EU body dealing with cyber security is the European Network and Information Security Agency ((ENISA), established in 2004. Its main task is to support member states, the European Commission, and the private sector in foreseeing, preventing, and responding to threats emerging in ICT networks. Some prerogatives in this area belong to the Joint Research Centre which, in 2010, organised with ENISA the first European simulation of a cyber attack.[33] The EU project called FISHA (A Framework for Information Sharing and Alerting) is also worth mentioning. Its main objective is to develop a European Information Sharing and Alert System, a pan-European system for sharing information relevant to the IT network data security.[34]

Also countries outside the Euro-Atlantic area do develop their potential in cyberspace. A good example of a modern approach to the ICT security issue is Israel. According to Israeli Military Intelligence chief Amos Yadlin, using computer networks for espionage is as important to warfare today as the advent of air support was to warfare in the 20th century and Tel Aviv has a military unit dedicated solely to carry battles in a cyberspace environment. Cyberspace has become a new tool in the hands of the IDF. In addition to military response teams fighting cyber attacks, Israel has also at its disposal specialists working for the intelligence of *Szin Bet, Mossad*, and - strikingly – for the Ministry of Finance. This, however, is not a complete list of entities involved in this particular dimension of the state security. In April 2011, Israel's government apparently planned to establish another special unit dedicated exclusively to combating acts of cyber terrorism. The unit would support the existing structures of Israeli intelligence. This information speaks for Tel Aviv being among world leaders in the field of cyber security solutions. The factor facilitating the development of Israel's potential is certainly the high advancement of technologies developed in this country, especially in the area of computer and communications systems security. It was probably Tel Aviv which developed the Stuxnet virus and successfully used it to compromise Syrian radars in September 2007, which proves the advancement level of Israeli solutions.[35]

---

[32] M. Chudziński, *KE boi się ataków DDoS*, "Dziennik Internautów" 06.12.2010, http://di.com.pl (acccessed 09.02.2011).

[33] M. Maj, *Pierwsza europejska symulacja cyberataku,* "Dziennik Internautów" 05.11.2010, http://di.com.pl (accessed 09.02.2011); *UE: Nowym prawem w cyberprzestępczość*, "Dziennik Internautów" 01.10.2010, http://di.com.pl (accessed 09.02.2010).

[34] *CERT Polska w projekcie FISHA,* "Dziennik Internautów" 01.04.2010, http://di.com.pl (accessed 09.02.2011).

[35] D. Eshel, *Israel Adds Cyber-Attacks to IDF,* "Aviation Week DTI" 10.02.2010; *Israel May Create Elite Cyber Security Unit*, eSecurity Planet, 07.04.2011, http://www.esecurityplanet.com (accessed

Apart from the United States, NATO and Israel, other actors highly relevant to cyberspace security are, of course, Russia and China. According to McAfee corporation experts, Russia and China are most advanced in their work on a "cyber weapon", i.e. a software capable of paralysing ICT networks of other countries. Although little information on the subject has been disclosed by their governments, some data has been published in the media and special reports. The approach of the Russian Federation to cyberspace has been aptly expressed by General Sherstuyuk who heads the Russian Institute for Information Security Issues. While interviewed about whether Russia has been working on the development of a cyber weapon, he replied: "It is not only Russia. It's just the 21st century. It is because of the high technology." As the former general said, Russia's IT security policy is mainly focused on combating threats posed by terrorist groups. It is true that the Russian cyberspace has not yet experienced serious acts of cyber terrorism, but -as he said - a serious threat is the use of the Internet by organised groups of fundamentalists to recruit new members and organise and plan assaults.[36] In fact, the Russian Federation has been one of the first countries to propose signing an international agreement on arms control in cyberspace.[37] It is known unofficially that Russia has been long developing its offensive capabilities in cyberspace. The Russian potential was demonstrated by events in Estonia, Georgia and Kyrgyzstan, where Russia proved that it belongs to world powers in this field. Kevin Coleman, an expert of DefenseTech, while referring to the problem, stated that "Russia has advanced capabilities […] necessary to carry out a cyber attack anywhere in the world at any time.". He believes that the Kremlin allocates ca. USD 127 million to its Cyber Warfare Budget annually and employs approximately 7300 experts as its cyber force. According to Coleman, its strongest assets consist in the BotNet and the advanced malware, including viruses and worms ("cyber logic bombs"), Trojans, and other tools designed for e-espionage.[38] Russia's activity in cyberspace is based on the so-called Russian Business Network, which controls the world's largest BotNet with between 150 and 180 million nodes, according to DefenseTech. This again proves Moscow's great potential in cyberspace.[39]

China has a similar potential proved by its capability by carrying out several, successful attacks on US networks in public and private sectors. As in the case of the Russian Federation, there is little official information on China's cyber security policy. First of all, it should be noted that the PRC is one of the few countries where the usage of the Internet is very highly controlled. The basic principle of China's

---

08.04.2011); D. Lev, *Experts: Israel's Cyber-Defense Can Stop Stuxnet Worm,* "Israel National News" 04.10.2010, http://www.israelnationalnews.com (accessed 08.04.2011).

[36] D. Talbot, *Russia's Cyber Security Plans,* "Technology Review" MIT, 16.04.2010.

[37] J. Markoff, A. E. Kramer, *In Shift, U.S. Talks to Russia on Internet Security,* "The New York Times" 12.12.2009.

[38] K. Coleman, *Russia's Cyber Forces,* DefenseTech, 27.05.2008, address: http://defen-setech.org (accessed 04.02.2011).

[39] K. Coleman, *Russia Now 3 and 0 in Cyber Warfare,* DefenseTech, 30.01.2009, http://defensetech.org (accessed 05.02.2011).

cyber security policy is, at least officially, to combat computer incidents and illegal and malicious software. Only in 2010, over 460 people were arrested there and charged with participating in computer hacking. Beijing has also supported a number of international initiatives aimed at controlling the use of the Internet, to mention the Resolution 57/539 of the UN General Assembly on *Creation of a global culture of cybersecurity*. Another manifestation of China's activity was the 2009 ASEAN-China framework agreement on network and information security emergency response.[40] At the same time, China's white information needs to be distinguished from actions actually taken by China. According to DefenseTech experts, today China's potential in cyberspace is the second highest in the world. Although only around 55 million dollars is allocated to its development, this is compensated by a large group of top IT experts working for the government, i.e. about 10 thousand people. According to Kevin Coleman, the strongest assets of the Chinese potential, as in the case of Russia, include: advanced large BotNet and highly advanced malware of all types. Furthermore, in his opinion, it is China which now is the most serious threat to cybersecurity of Western countries.[41] The growing capabilities of the PRC can be further proved with the Chinese plan of action in cyberspace in the event of war against the United States, disclosed by "The Sunday Times." The plan includes not only crippling US financial or ICT capabilities but also for paralysing the US aircraft battle carrier fleet with a cyber attack.[42]

One should also remember that both Iran and North Korea have increasingly larger capabilities in cyberspace. The regime in Pyongyang has repeatedly been accused of carrying out attacks against South Korean and US websites. The most serious attack took place in July 2009. It is estimated that 18 thousand computers and 11 government websites were infected in South Korea alone. According to the American Enterprise Institute's expert Nicholas Eberstadt, that attack has proved that North Korea tries to complement its nuclear potential with its offensive capacity in cyberspace.[43] It is estimated that Pyongyang employs about 12 thousand computer experts and spends around USD 56 million per year on its activities in cyberspace. Experts have ranked North Korea eighth among all countries with such capabili-

---

[40] *China's Cybersecurity and Pre-Emptive Cyber War*, China Defense Mashup, 13.03.2011, http://www.china-defense-mashup.com (accessed 04.02.2011); *China's Faltering Cybersecurity Efforts Offer Chance for Engagement*, China Defense Mashup, 10.12.2010, http://www.china-defense-mashup.com (accessed 04.02.2011).

[41] K. Coleman, *China's Cyber Forces*, DefenseTech, 08.05,2008, http://defensetech.org/2008/05/08/chinas-cyber-forces/.

[42] T. Reid, *China's cyber army is preparing to march on America, says Pentagon*, "The Sunday Times" 08.09.2007. More on the American-Chinese conflict in cyberspace in: C. Bartholomew, L.M. Wortzel, *Report to Congress 2009*, U.S.-China Economic and Security Review Commission; N. Hachigan (2001), *China's Cyber-Strategy*, "Foreign Affairs" March/April.

[43] D. Kirk, *What's behind cyber attacks on South Korea, US?*, "The Christian Science Monitor" 08.07.2009; S. Gorman, E. Ramstad, *Cyber Blitz Hits U.S., Korea,* "The Wall Street Journal" 09.07.2009.

ties.[44] The policy of Iran is similar and Iran is one of five states capable of waging war in cyberspace according to CIA. Operations of the Iranian Cyber Army (ICA) testify to the skills of Iranian experts. It regularly attacks US and European servers. During one of such attacks, in October 2010, the hackers targeted over a thousand French, British and American websites.[45] The ICA has one of the largest BotNet of around 400 thousand personal computers.[46] According to DefenseTech, Iran has about 2400 computer experts working for the Islamic Revolutionary Guards. Their budget is, according to Kevin Coleman, around USD 76 million.[47] Moreover, in early 2011, Iran established a special police unit dedicated to trace on-line crimes. That event also testifies to the advancement of Iranian solutions.[48]

## CONCLUSIONS

Cyber threats that have emerged along with the processes of computerisation and dissemination of the Internet, keep evolving. At first, there were relatively not serious incidents caused by home computer hackers. In the second half of the 1990's, however, computer security hackers or crackers emerged along with the growing interest of some countries in the potential of cyberspace. The use of cyberspace has facilitated operations the outcomes of which are extremely difficult to achieve using traditional methods. The factor strengthening this trend is a specific nature of ICT networks. In cyberspace, it is easy to remain anonymous, there are no traditional boundaries, and the cost of operations is low. In addition, there are uncertainties about the applicability of existing political solutions (e.g. alliance treaties) and provisions of international law to cyber threats. This makes some countries adventurous in cyberspace. The turning point for the perception of new security challenges were surely the years 2007-2008. Events which took place in Estonia, Georgia and Iran clearly demonstrated that cyberspace can be used to carry out actions aimed at disrupting basic functions of the state.

The potential of the ICT space was discovered first by the United States, then Russia and the People's Republic of China. Political strategies and technological solutions developed in those countries have provided not only for the use of cy-

---

[44] *North Korea Waging Cyber Warfare?,* CBS News, 09.07.2009, http://www. cbsnews.com (accessed 04.02.2011); C. Clark, *North Korea: Cyber Mad Dogs or Bluster Kings?,* "Dod Buzz" 20.04.2009, http://www.dodbuzz.com (accessed 04.02.2011).

[45] *Iran's Cyber Army Hacks 1,000 US, British, French Govt Websites,* FARS News Agency, 30.08.2010, http://english.farsnews.com (accessed 04.02.2011).

[46] *Irańska Cyber Army tworzy botnet,* "Dziennik Internautów" 31.10.2010, http://di.com.pl (accessed 09.02.2011).

[47] K. Coleman, *Iranian Cyber Warfare Threat Assessment*, DefenseTech, 23.09.2008, http://defensetech.org/ (accessed 04.02.2011).

[48] *1st Cyber police unit launched in Iran*, Press TV, 24.01.2011, http://previous. presstv.ir (accessed 04.02.2011).

berspace for defensive purposes (such as critical infrastructure protection), but for offensive actions as well. Already in the 1990's, the United States recognised potential problems stemming from the dynamic computerisation and "informatisation of life". This was mainly due to the fact that already at that time, the US was the most frequent target of hacking attacks. This resulted in a relatively prompt launch of research that accurately foresaw further development of cyberspace and the specific character of actions taken in this dimension (including, inter alia, legal and political controversies).[49] What is also important, the US was one of the few countries which took concrete steps in this area before Estonia and Georgia were attacked. The US created the first military command for cyberspace which, with time, will provide the US with capabilities adequate for using ICT networks in conditions of armed conflict. Thus, the US is certainly the leader in the field of innovative cyber security solutions.

Other countries in the Euro-Atlantic zone have certainly been inspired by the American experience and solutions. Poland's cyber security policy started to emerge after the crisis in Estonia. The experience of the government in Tallinn made Polish secret service take steps to evaluate the security of government servers. They were conducive to the development of the first government document which comprehensively covered the issue of the cyberspace impact on national security. Poland's solutions in this area have been largely based on the experience of the United States and other European countries. In addition to creating an institution responsible for the protection of government networks (CERT), which is now a standard procedure, Warsaw has also established the first Polish military unit designed to operate in cyberspace, which should be considered a substantial success. Poland's *Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016* has set the path for future undertakings. For quite inexplicable reasons, however, Polish secret service showed no interest in participating in the CCD CoE in Tallinn.

As far as allied countries are concerned, certainly one of the most advanced is Israel. Despite little official information on Israel's cyber security policy, the potential of Tel Aviv can be assessed on the basis of its use of IT potential against countries in the Middle East. Using a virus to blind Syrian radars was the first ever military operation, the success of which was primarily due to the use of ICT technologies. Definitely more important, however, was the development of the *Stuxnet* virus software. According to experts, the use of this virus against Iran is comparable to the explosion of the first nuclear bomb[50]. The *Stuxnet* software has been the most advanced and sophisticated cyber weapon ever created and marked a new stage of "arms race" in the cyberspace environment. Its importance has been confirmed with slowing down the Iranian nuclear programme and that is a success.

---

[49] Cf. B.W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, U.S. Army War College Strategy Research Report, 10 April 2001.

[50] *Stuxnet heralds age of cyber weapons, virtual arms race,* "Homeland Security Newswire", 27.01.2011, http://homelandsecuritynewswire.com (accessed 01.03.2011).

Interestingly, international organisations seem to take much less action. Among them NATO is surely an organisation that has advanced solutions in the field of cyber security. First and foremost, this is due to the attack on Estonia which has resulted in the inclusion of this security dimension in NATO's new strategic concept. In spite of the above, however, it should be noted that solutions proposed by the Alliance are quite limited. This is due to little coordination between NATO member states and serious questions of political and legal nature. The use of ICT networks still eludes traditional political/legal solutions on which the functioning of the Alliance is based. NATO has developed mechanisms to assist its attacked members. The mechanisms, however, do not directly follow from provisions of the North Atlantic Treaty. Cybersecurity is of definitely lesser importance in the EU's Common Foreign and Security Policy. The EU has only recently recognised the significance of cyberspace and its solutions in this field are underdeveloped.

The Russian Federation should be regarded as a forerunner of massively using the new security dimension to gain political profits. Thrice in recent years, Russian computer experts carried out cyber attacks against the network infrastructure of neighbouring countries, each time achieving their objectives. Their victory in the three "cyber wars" proved that today Russia is one of the greatest global powers in cyberspace. Moreover, in contrast to countries of the Euro-Atlantic zone, Russia uses cyberspace primarily to execute its interests in the international arena. China's policy has been similar. Since the late 20th century, China has been involved in majority of most serious cyber attacks (*Aurora, Titan Rain*). However, unlike the Russian Federation which specialises in acts of cyber terrorism, the PRC is famous mainly for its cyber espionage. Most of well-known Chinese hacking attacks have primarily been aimed at stealing classified information of a political, economic, or military character. One should also bear in mind that Iran and North Korea become increasingly important players in this area. Their Internet activity has, so far, been little, yet their growing potential may pose some risk in the future.

To summarise, processes of computerisation and digitalisation underlying the development of cyberspace, despite the benefits, will constitute an increasingly serious threat to national security. This has been confirmed with the events in the early 21st century, when first cases of the offensive, massive use of the Internet were recorded. A proper perception of and response to cyber threats have now become a most serious challenge to security policies of national governments. The response time to new challenges and the most appropriate path of development of the potential in this area will determine not only the security but to some extent also the status of particular countries on the international arena.

ABSTRACT

*The article tackles the problem of sensitivity to threats that appear in cyberspace in the security policies of selected international actors, including e.g. the USA, Poland, Israel, Russia, the European Union and the North Atlantic Treaty. Cyber threats have intensified with the development of information technology and the popularisation of the Internet. Initially they were not very serious attacks carried out by self-taught programmers. Since the mid-1990s, the character of hackers' activity has changed along with the growing interest of individual countries in cyberspace issues. Many countries, including the USA, Russia and China, began to focus on the development of their potential in this area in order to ensure maximum protection of their critical infrastructure against cyber-attacks. In the 21st century, the significance of cyberspace for international security keeps increasing. The promptness of response to new problems and the most appropriate path of development of the potential in this area will, in the future, determine not only the security but to some extent also the status of particular countries on the international arena.*