Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-687-692

CYBER SECURITY AS A GLOBAL CHALLENGE TODAY

Žaklina Spalević
Singidunum University, Serbia

Abstract:
Cyber space is a virtual unowned computer creation, which requires a high level of technical equipment and a good information infrastructure. This space without national boundaries simultaneously coexists with a real space in order to make collective communication among people faster and better. Nowadays cyber culture is evolving faster than technologies in the field of cyber security, so the private data, intellectual property and resources of conventional civilian and military infrastructure may be compromised or damaged by the deliberate cyber attacks, unforeseen to security flaws and internal vulnerability of the Internet. Cyber warfare is a form of latent aggression committed by one state or organized crime groups in order to weaken the economic and military resources of another state that is the target of the attack. In this regard, the unresolved issues of cyber security create an imbalance between state security and human security, which is particularly evident in the case of financially powerful individuals who have specific personal motives and priorities. The basic model for effective monitoring and improving cyber security and protection of the right to privacy, freedom of expression and association is a public-private partnership.

Key words:
Cyber Space,
Cyber Security,
Cyber Warfare,
Latent Aggression,
Cyber Security Strategy.

INTRODUCTION

Major technological advance in the field of information and communication technologies has lead to the emergence of new forms of crime acts that could not be followed by and included in syber crime regulatives, indicating that the cyber crime phenomenon which comes with technological development is beyond the social, ethical, legal, political and other frameworks that exist in a social community.

Cyber crime is a crime that relates to any kind of crime that can be done with, in, or against computer systems and networks. In fact, cyber crime takes place in electronic environment, causing the need for the co-called cyber culture and cyber security.

Despite the fact that cyber culture and security appeared in almost same instance of time as cyber crime, cyber culture is evolving faster, leading to problems because everything that depends on cyberspace is subject to certain risk. The global economic crisis intensifies the a forementioned risk.

CONCEPTUAL DEFINITION OF CYBER CRIME

Difficulties with the conceptual definition of cyber security resulte from the fact that in most cases it is extremely hard to accurately identify the attackers and the country they originated from [1], which indicates that cyber security represents a global challange today.

Furthermore, owners of information and communication networks are mainly private individuals [2] and security of these networks are being granted by the governments in each of the state. In this regard, one of the key challanges of cyber security is reflected in the fact that mentioned subjects have specific interests which impede efficiency and impact of efforts in the field of cyber security.

In order to work together on the whole, a transnational, solution that goes beyond the technology and be able to fight with all the threats against the comprising deliberate cyber attacks, unforeseen to security flaws and internal vulnerabilitis of the Internet, one country's Governments should become partner to private sector, citizens and other Governments. Above mentioned shows that cyber security includes challanges that are beyond national borders, while answers to these challanges, which are usually insufficient, remains overwhelmingly national in scope.

DEMOCRATIC OVERSIGHT OF CYBER SECURITY POLICIES

Countries in the world are faced to many traditional and non-traditional security challanges and inability to continuosly equipe their services with modern information and communication resources. As the result, there is a clear need for cooperation between the public and private sector in order to establish democratic control policies of cyber security[3].

In this regard, one of the answers to the current challanges of cyber security is the model of 'management network', which allows delegation or transfer of resposibilities in the field of minitoring the cyber security in two directions. In one direction, countries are indicated to companies, while in the other companies are indicated to coutries (eg. the recent cooperation agreement between Google and U. S. National Security Agency (NSA), in order to help this company to secure its network after recent attack by Chinese hackers). Exeptional advantage of management networks is reflected in the fact that they involve cooperation between governments, private sector, non-governmental and international organizations, as well as the fact that all users are able to use geographical, technological and scientific resources, that they themselves would not be able to provide. However, appearance of management networks contains many, not only theoretical, but practical challanges that are not yet been thoroughly explored.

Issues of this nature are particulary present in the field of public-private cooperation, because the same is often not transparent and that the activities of certain parts of the management network are often complex and hidden from the monitoring bodies and institutions of democratic governance [3]. On the other hand, despite the fact that in the cyber security field are involved a large and diverse number of public, private, international and other non-state subjects, follow-up of participants in the cyber attacks is very difficult due to large and diverse number of them. All this makes it difficult to acquire furhter knowledge about organized groups and individuals performing cyber attacks and all activities which are undertaken by cyber attacks.

Apart the problem emerging from insufficient research of management networks and their own complexity, there are numerous other factors that exacerbate the democratic monitoring of the cyber security policy. One of these is the fact that because of the highly technical nature of the cyber security challanges and responses to them, monitoring bodies often lack the necessary skills to understand and adequately monitor them.

Quite apart from the technical complexity, complexity of legal matters worsens the monitoring as well. In the field of democratic control of cyber security policy, the most complex legal issues are those relating, on the one hand, the right to privacy and freedom of expression, and on the other side the right to public-private cooperation and related legal issues in the terms of their resposnability and control.

Heterogeneity of the participans in democratic oversight of cyber security policy makes its implementation difficult. In most cases, monitoring insistutions are organized as agencies or funcionaly similar bodies (eg. parliamentary committee can monitor the work and activities of the intelligence services, armed forces and the judiciary). However, public-private cooperation required by cyber security policy is spread across agency boundaries, even beyond thir mandates. The consequences are reflected in a number of areas in which the policy of cyber surveillance is not implemented or is inadequate.

Perceptions of mandates also create problems in the field of democratic control of the cyber security policy. Seen from a broader point of view, government monitoring bodies are concerned with the government agencies whose activities are directly responsible for. That leads us to conclusion that government monitoring does not include monitoring of private partners of government agencies, even in the cases when they are directly funded by them.

The issues of democratic monitoring of cyber security policy is further complicated by the global nature of 'the networks involved'. Unlike conventional forms of crime, cyber crime is characterized by significantly expanded scope of the criminal acrivities that do not require the presence of the offender to the crime scene. In most cases, the offender is in one country, crime scene in second, and consequences of crime take place in third country. Suitable area for the commission of cyber criminal acts are countries where there is no legal framework, or there is partial legal framework in the fight against cyber crime.

In the field of democratic monitoring of cyber security policy, effective cyber security faces the same limitations as does other forms of international cooperation, especially with added complexity of involvement and resposibility of the private sector in national legislation. Forth suggests the need to establish common strategy and standards at the international level. However, efforts to foster international cooperation will inevitably face the challenge of anonymity balancing, privacy and openness with efforts to share information and better detection, prosecution of perpetrators of cyber crime.

CYBER WARFARE AS A FORM OF DISGUISED AGGRESSION

Insight of cyber warfare area requiers complex and multidisciplinary approach and development of new, original and effective principles and norms in the construction of national and collective cyber security strategy, as well as development of specific technological and legal instruments for its implementation [4,5].

The use of electronic communication and computer resources in cyber space allows the enemy the possibility to simultaneously launch operations from the various points on the globe, that way masking its military operations to forms of crime or terrorism committed by unknown perpetrators, disturbing the status and rights of the neutral parties in the conflict [6].

The fact that cyber warfare is performing using the same tools, techniques and methods used in the field of cyber crime, terrorism and intelligence activities is indicative of very specific nature, which allows states to launch covert attacks on opponents. In this regard, the starting point in defining doctrine, procedures and standards in the field of cyber warfare is to determine its true nature. Understanding the real nature of cyber warfare is a necessary condition for building national capatities for cyber warfare, which are military justified and consistent with international law.

In order to understand the concept of cyber warfare it is necessary to clearly define the difference between 'war' and 'warfare'. In principle, 'war' is a state of hostility or conflict, usually open, published and armed conflict between countries or nations, the basis of which is armed struggle, but also other forms of conflict (political, economic, propaganda, psychological). Unlike war, 'warfare' is a process or acrivity that is conducted between the opposing sides who are in a state of war, assuming use of of both arms and methods for conductiong war activities, and can be understood in a broad and narrow sense [7].

In a broader sense, the warfare means a wide range of military and non-military activities directed against the rival, in order to impose one's will [4]. In a narrow sense, the warfare refers only to the use of military or non-military methods in a specific field, such as law, information technologies, cyber space, from where the term 'cyber warfare' had been derived.

Having in mind narrow and broader sense of warfare, one can conclude that it is not limited to the use of weapons, but also the application of other, directly non-lethal means, methods and technique and that in case of conflict in cyberspace it is more appropriate to speak of warfara than of war.

In order to achieve adequate legislation of cyber warfare, it is necessary to define the concept of cyber weapons, which has a broad meaning. Generally speaking, it means any program, technique or device that can be used to access opponents systems for the purpose of military action against them.

In order to devise the nature of cyber warfare it is necessary to make an analogy to the firearm. The U.S. Department of Defence defines the term 'firearm' as a 'tool intended to kill, hurt or incapacitate people or to damage or destroy material resources'. After firing a shot, bullet is passing through the air and hits the target, that way destroying it. Weapons, by itself, do not create damage, but have the purpose to supply the means of destruction (bullet) to the target [8].

The mean of destruction makes no damage unless it is fired by firearm. In the end, neither weapons, nor bullet are not dangerous unless the fighter takes them, load the weapon with bullets and takes a shot. In cyber warfare, malicious code, computer instruction or date are the means of distruction and act as a bullet. Computer hardware is the means by which this 'bullet' is being created and delivered to the target of the attack. Operator who used information systems, or programmer who writes programs by which cyber attack is being performed is the fighter.

Therefore, the three elements are the basics of cyber attack: software, hardware and the fighter. Each of them is of importance to war law for regulation of war conflicts. They have to be used in accordance with the principles of the law of armed conflict, and the fact that they are used for armed conflict makes them legitimate target of attack. In order to provide answers to the question of whether cyber attack has the exclusive nature of cyber warfare, that is, whether an act of aggression starts from the Resolution No. 3314 UN General Assembly on December 14., 1974. [9,10], according to which aggression is defined as 'the use of armed force by a state against the sovereignty, territorial integrity or political independece of another state', and which points to the conclusion that cyber warfare is, too, a form of aggression. While not included under any of the acts of aggression, Cyber warfare is an offence directed against the sovereignty, territorial integrity and political independence of states committed by other countries which usually conceal their actions, and because it is not committed by conventional armed forces whose effects are clearly visible, has a covert form of aggresion [11]. Outlined points to the necessity to accept cyber warfare on an international level, as well as necessity to establich appropriate legislation, after which its criminalization as a crime of aggression [11,12].

CYBER SECURITY POLICY IN THE WORLD

The fact that today cyber culture is developing faster thatn technologies in the field of cyber security has resulted in a number of countries in the world focusing on establishing and further development of adequate cyber security policies, both internally and internationally.

Testimony of the outlined is establishment of an Operational center for cyber security in Australia in order to protect the informational infrastructure (CIP) and critical informational infrastructure (CIIP) 2009., based on the government's strategy for cyber security. This center is managed by the Defence Signals Directorate (DSD), which corresponds to a parliamentary committee for security.

In Canada, the Canadian Centre for responding to cyber incidents (CCIRC) is responsable for monitoring the cyber space, protection of critical national infrastructure and coordinating the national response to any form of cyber security incidents. This center, also, coordinates the work of the special department of the Communications Security Establishment and the Canadian Security Intelligence Agency to deter cyber threats. The Canadian government in February 2010. brought a detailed five-year action plan for the adoption of the National Strategy for Cyber Security in order to enable the country's ability to cyber warfare.

Institutional Security Cabinet (GSI) coordinates system to protect critical information infrastructure (CIIP) in Brazil. Governments safety activities in cyber space is managed by the Committee for Security Information Management. The same is composed of representatives from all ministries and state police for information communication Technologies. ANATEL (the federal telecommunications regulatory body), SERPO (federal service for data processing) and CERT (computer emergency response team) are working together in order to improve and deepen the joint action of public and private sector in provision of IT infrastructure.

There is no special government body resposible for CIP/ CIIP in Austria, but each ministry implements specific measures to defend against external cyber attacks and prevent unauthorized use of data. The central authority for public security in the federal criminal police is leading the fight against internet child pornography. Second section

of the ministry of defence is responsable for all aspects of cyber warfare. Several departments of the ministry of the interior (BMI) are dealing with CIIP, that is data security and criminal offenses in the area of cyber crime.

Belgian ministerial committee on security and intelligence has the ultimate responsibility in forming of national informational security. Commision for the protection policy provides protection of personal data, while the Belgian Institute for postal serveces and telecommunications offenses is responsable to ensure compliance of by-laws acts with the law of electronic communications and their implementation.

In Germanu, the National plan for information infrastructure protection (NPSI) presents a fundamental politico-strategic document for the protection of itnerests kept in cyber space. On its basis, at june 2009., National strategy for critical infrastructure protection (CIP) was consituted, which summarizes the goals and intentions of the government in the next ten years. Federal office for information security (Bundesamt für Sicherheit in der Informationstechnik [BSI]), as a part of the Ministry of internal affairs, developes assessment and analysis of cyber threats and protection concepts, together with the Federal office for civil protection and disaster assistance (BBK), the Federal criminal police (BKA), Federal police (BPOL) and the Federal institute for technical support.

French parliamentary system is characherized by considerable powers of the president in a crisis situation. It is therefore not surprising that the General secretariat of national defense (SGDN) was established at the office of the prime minister and bears a complete responsibility for the organization of the CIP. In France, cyber security is seen as resulting factor that affects the development of the informational society in the presence of daily threats and activities of organized groups in the field of high-tech crime. In France, in july 2009, National agency of the security of information systems (ANSSI), which is resposable for CIIP and cyber security, was established with the Ministry of defence. In order to develop public-private partnership in the field of protection of national interests in cyberspace, the Strategic advisory board on informational technologies (CSTI) seeks to provide a coordinated action with representatives of government, industry capacity, representatives of business and scientific research organizations.

The United Kingdom has stressed the need for a coherent approach to cyber security through Cyber security strategy, brought in 2009. Roles in this strategy have government, all economic actors and international partners of the state. Office of the cyber security (OSC) with the office of the prime minister should provide strategic leadership and coherence of all capacities of ministry od defence, intelligent agencies and police (metropolitan police for e-crime, Centre for online protection from child abuse and the Serious organized crime agency - SOCA) in the case of cyber attacks. Center for Cyber security management (SCOC) is located in the Government communications headquarters (GCHQ) in Cheltenham and combines the funcions of monitoring cyberspace, coordination of response to incidents and provides a better understanding of attacks against UK networks and provides advice and informations on the risks of businesses and public subjects in cyberspace.

Ministry of Interior (Police service of postal communication) and the Ministry of innovation and technology are the main public authorities in Italy, dealing with the issue of CIIP. Police official postal communication is managing by emergency centers at both the national and regional levels, in order to fight cyber crime more efficient. In order to improve CIIP at all levels, public agencies also work closely with the private sector. Association of Italian experts for critical infrastructure and experts group of experts from the public and private sectors are two main forms of public-private partnerships in the field of CIP in Italy.

In 2007., Estonia was subjected to a series of DdoS attacks that resulted in shutting down the website of the Ministry of foreign affairs and the Ministry of justice, temporary blocking of national emergency phone line and websites of State and Federal election commission. As a result, Estonia had adopted the Strategy for cyber security in 2008., that way defining the policy of impoving cyber security. The main task to define the CIIP was assigned to Ministry of economy and communication (MEAC), which coordinates the work of the Department of state information systems (RISO) and the Estonian informatics centre (RIA), as well as the work of central agencies for national IT policy.

Finland comprehended term of cyber security as issue of data security and development of the information society as a state economic devlopment issue. Finland established three major state agencies to deal with CIIP: Finnish communications regulatory authority (FICORA) in the Ministry of transport and communications (main task of this agency is to promote the information society and to work on technical regulation and standardization), National emergency supply agency (NESA) (main task of this agency is to analyze the threats and risks of CII) and the Steering committee for data security in state administration (VHATI) (develops policy guidelines and practical guide to IT security systems). In the field of state-private partnership in order to develop CIIP, National emergency supply council (NESC), Comprehensive information society advisory board and the Finnish centre for development of the information society (TIEKE) were established.

In Hungary, through the Electronic government centre, Prime Minister's office coordinates the activities of e-government and other CIIP contents. The Ministry of defence is responsible for national security, including the security of information of national importance. Ministry of justice and law enforcement is responsible for the prevention of cyber crime, data protection and control of the state administration and the Central electronic public services.

The European Union is an important international factor who has launched a range of initiatives and research programs in order to study various aspects of the information revolution and its impact on education, business, health and communication. CIIP, CIP, information security and the protection of privacy on the Internet is one of the priorities of the EU policy.

NATO started its cyber defence program in 2002., after successful actions of Serbian hackers who had managed to get into Information system of NATO in Brussels. For one week no one at the headquarters of NATO had been able to send emergency e-mails or to use the Internet. During the aggression against Yugoslavia, NATO's information system was exposed to attacks by Serbian and Russian cyber warriors, causing the leakage of information to the Yugoslav army.

Bearing in mind the experience in fighting Serbian Internet warriors, NATO leaders ordered implementation of technical NATO cyber defence program at their summit in Prague in 2002., which started by establishing NATO Computer incident response capability (NCIRS).

The capacities of NCIRC coordination centre at NATO headquarters in Brussels and NCIRC technical centre in Mons, NATO possess the means to carry out the key tasks, from detection and prevention of computer viruses and unauthorized intrusion in NATO's networks, to the management of cryptographic devices on the Internet.

Problems of CIIP have been one of the most frequent issues in the United Nations since late eighties, but the formal progress in area of CIIP in UN is recent. This progress is reflected in the initiatives of the Forum for security and democracy, which has been led by the UN institutions, several adopted UN resolutions and the results of the World summit in the information socitety (WSIS).

Increased number of cases in the field of cyber crime has specific consequences to the financial sector. Considering the growing amount of financial data that is stored and transmitted online, the ease with which it can be broken into computers only makes the problem more severe. Therefore, the World bank has taken several steps over the last few years, in order to deal with the challanges of information security, particulary i developing countries.

In 2007., team for Strategic dialogue of East-West Institute (EWI), led by retired U.S. general James Jones, called in discrete discussions high russian and chinese officials to break deadlock in international cooperation in dealing with cyber challanges. Intensive consultations have followed on high level double track.

All three governments confirmed their concern about the intentions and actions of others. It has been shown that there is a deep-seated concern about the increasing capacity of non-state sector, which is able to distroy the world's economic stability, and that could pose a serious security challange. All three countries have changed their assessment of the importance of cyber security, which the U.S. even raise to the level of nuclear safety [14].

U.S., China and Russia at the World cyber- security initiative (WCI) which is managed by the East West Institute actively cooperate in order to achive better security in cyber space. They were joined by leading figures from the EU and other G20 countries, the private sector, professional associations and international organizations.

CYBER SECURITY CHALLENGES IN SERBIA

In Republic of Serbia, listening or control of the flow of information of nearly 400.000 people occurs on daily basis, of which only 15.000 legal, while others are under unautohorized supervision of either public authorities, individuals, private agencies or agencies. This leads to the conclusion that the monitoring of cummunications has reached unimaginable proportions and that it is necessary to establish a serious control system in the form of establishing democratic politics in the future [15].

Conducted studies have shown that in Serbia every mobile providers can activate the software application that registers the frequency of eavesdropping, and that there were more than 270.000 accesses by security services and police to so-called detained data communication, that is to data which contained information about who, when, how, where, with who, how long had spoken.

This data, bearing in mind number of providers in Serbia, leads to the assumption that such approaches had taken place in more than hundreds of thousands, even million times. Bearing in mind that these approaches are unacceptable by the Consititution of Serbia, urgent reaction of state authorities is necessary in order to find an adequate answer to the above mentioned challenges of cyber security. One of the first steps on this path is a strict ban on the police to collect data without a court order, as the unauthorized interception is a criminal offense and as such must be recognized [16]. In this regard, in unauthorized wiretapping not only take placy national service, but also providers.

Interception problem should not be reduced only to a possible unauthorized wiretapping performed by authorized services, police, BIA (Security Information Agency of Republic of Serbia) or VBA (Military Security Agency of Republic of Serbia), because the same occurs as well in the so-called 'grey area'. Because of the lack of legislative regulation in this area in Serbia, structures of the world of business, politics and crime can perform wiretapping, nowdays [17].

This also means that parties, companies and individuals can have the so-called *services for tracking*, which points to the fact that the Republic of Serbia anyone can be blamed for the abuses in the collection of secret data. All together confirms the conclusion that it is necessary to establish democratic politics of cyber security in the Republic of Serbia.

CONCLUSION

The rapid progress in the development of information and communication technologies and the Internet, and their grown impact on social phenomena and processes have led to increased interest in all phenomena arising from this development. One of such phenomenon is cyber warfare. Area insight into cyber warfare requires complex and multidisciplinary approach to the development of new, original and efficient principles and norms in the construction of national and collective cyber security strategy and specific technological and legal instruments for its implementation.

In order to uniquely regulate area of cyber security and set directions for successful operation in the future, states (as well as international community) should behave as re-

sponsable members of the international community and should act in accordance with existing international law. In order to accomplish this in the area of cyber security, is that the national legislation and doctrine fully understand its essence and nature.

Only in that case it is possible to build a comprehensive national strategy and doctrine to establish democratic politics of cyber security and to provide a national contribution to international efforts in orders to create a specific legal framework in this area.

REFERENCES

[1] J. Markoff, D. E Sanger and T. Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent", The New York Times, January 25, 2010; Internet Source: http://www.nytimes.com/2010/ 01/26/world/26cyber.html, Date of view: 9.12.2013.

[2] J. Wood and B. Dupont, eds., "Democracy, Society and the Governance of Securityv, Cambridge: Cambridge University Press, pp. 78-81, 2006.

[3] A. Bailes, "Private Sector, Public Security", in Private Actors and Security Governance, A. Bryden and M. Caparini, Eds. Berlin: Lit Verlag, pp. 42, 2006.

[4] R. Szafranski, "A Theory of Information Warfare: Preparing for 2020", Air & Space Power Journal, Vol. 9, No.1, pp. 56-65, 1995.

[5] S. Gorman, J. E. Barnes, "Cyber Combat: Act of War", The Wall Street Journal, 31 May, 2011; Internet Source: http://www.online.wsj.com/article/ SB10001424052702304563104576355623135782718.html, Date of view: 9.12.2013.

[6] International Strategy for Cyberspace, The White House, May 2011; Internet Source: http://www.whitehouse.gov/sites/default/files/rssviewer/ international strategycyberspace.pdf, Date of view: 9.9.2013.

[7] D. D. Mladenovic, D. M. Jovanovic, M. S. Drakulic, "Defining of Cyber Warfare", Military Technical Courier, Vol. 60, No. 2, pp. 84-117, 2012.

[8] D. Vuletic, "Defending against Threats in Cyber Space", Strategic Research Institute, Belgrade, pp. 70-71, 2011.

[9] Report of the Working Group on the Crime of Aggression, Review Conference of the Rome Statute, International Criminal Court, 2010.

[10] Rome Statute of the International Criminal Court, U.N. Documnet A/CONF.183/9, 17 July 1998.

[11] Z.Stojanovic and D. Kolaric, "Aggression in the International Criminal Law", Proceedings of XII International Scientific Conference: International Criminal Acts, pp. 39-55, 2013.

[12] The crime of aggression resolution of the International Criminal Court, RC/Res.6, adopted at the 13th plenary meeting, on 11 June 2010.

[13] B. S. Buckland, F. Schreier and T. H. Winkler, "Democratic Governance – Challenges of Cyber Security", Forum for Security and Democracy, Belgrade, 2010.

[14] K. F. Rauscher, A. Korotkov, "Russia-U.S. Bilateral on Critical Infrastructure Protection: Working Towards Rules for Governing Cyber Conflict", East-West Institute, pp.36-37, 2011.

[15] M. Kostic and V. Vilic, "Measures for protection the right to privacy according to Council of Europe Convention on Cybercrime", Proceedings of the Faculty of Law, Vol. 63, pp. 83-93, 2012.

[16] The Law on Electronic Communications, Official Gazette of the Republic of Serbia, No. 44/2010 and 60/2013 - Decision of the Constitutional Court.

[17] U. Misljenovic, B. Nedic and A. Toskic, "Privacy Policy in Serbia - Analysis of the Law on Protection of Personal Data", Partners for Democratic Change Serbia, pp. 7-9, 2013.

CYBER BEZBEDNOST KAO GLOBALNI IZAZOV DANAŠNJICE

Abstract:
Cyber prostor predstavlja virtuelnu računarsku bezvlasničku tvorevinu, koja zahteva visoku tehničku opremljenost i dobru informacionu infrastrukturu. Ovaj prostor bez nacionalnih granica paralelno koegzistra sa realnim prostorom u cilju brže i kvalitetnije kolektivne komunikacije među ljudima. Cyber kultura razvija se danas brže od tehnologija u oblasti cyber bezbednosti, tako da se privatni podaci, intelektualna svojina, kao i resursi konvencionalne civilne i vojne infrastrukture mogu kompromitovati ili oštetiti namernim cyber napadima, nepredviđenim sigurnosnim propustima i unutrašnjom ranjivošću Interneta. Cyber ratovanje je vid prikrivene agresije, počinjen od strane jedne države ili organizovanih kriminalnih grupa u cilju slabljenja privrednih i vojnih resursa države koja je meta napada. S tim u vezi, nerešena pitanja cyber bezbednosti stvaraju disbalanse između bezbednosti države i bezbednosti pojedinca, koji je posebno izražen u slučaju finansijski moćnih fizičkih lica koja imaju specifične lične motive i prioritete. Osnovni model za efektivno poboljšanje i nadzor cyber bezbednosti, kao i zaštitu prava na privatnost, slobode izražavanja i udruživanja predstavlja javno-privatno partnerstvo.

Key words:
Cyber prostor,
Cyber bezbednost,
Cyber ratovanje,
prikrivena agresija,
Strategija Cyber bezbednosti.