THE VALUE CHALLENGE OF INTERCONNECTEDNESS IN CYBERSPACE FOR NATIONAL SECURITY

Dragan Ž. Đurđević[1],
Miroslav D. Stevanović[2]

[1]Academy of Nacional Security;
Belgrade, Serbia

[2]Security Information Agency,
Belgrade, Serbia

Abstract:

The current phase of the information age is characterized by more intense and more comprehensive interconnection in cyberspace. This feature of technology promotes changes at the societal level, including consequently the value model. These changes require adaptation of national communities and, thus, represent a challenge for the national security.

This paper starts from the observation of parameters of interconnectedness of things, people and processes in cyberspace, and their impact on social organization within the technologically advanced states. That impact is analyzed in regard to the stability of the common value concept of nation-states.

The interconnectedness in cyberspace manifests the trend of multiplication in scope. In the leading technological countries, centralized development centers are emerging. This results in attracting financial flows towards the most developed countries, and the rise of the technological elite as an actor in the social power structure.

Adapting to the interconnectedness (and the speed) in cyberspace requires improving the individual capacity of perception, which can be achieved through value-oriented education. Re-composition of social power within the community requires implementing democratic mechanisms in cyberspace, and the precondition for this is a strategic national approach to protection and normative regulation of critical information infrastructure.

Key words:

interconnectedness in cyber space, the Internet of things, start-up technological center, capacity of perception, national cyberspace protection strategy.

1. INTRODUCTION

The development of information technologies has enabled a global network of interconnected users, but also a global network of interconnected, uniquely identified objects (Internet of Things, IoT) [1]. The exchange of data between things, as well as between things and people, in cyberspace requires the standardized "language" of communication, an internet connection as a means that enables communication, and an internet protocol with adequate capacity to span an unpredictable number of potential participants in communication (IPv6 address).

A global network of two global networks (the Internet and the IoT) will necessarily induce changes in at least three aspects of human environment: firstly, more extensive and more intensive networking of people and things, secondly, in organization of management of human communities,

Correspondence:

Dragan Đurđević

e-mail:

djurdjevic.dragan@gmail.com

DOI: 10.15308/Sinteza-2016-15-23

in bureaucratic as well as within the urbanization concept, and thirdly, business and services.

Global network, however, remains in the domain of tools, resources and means that increase human possibilities. As such, in order to ensure improved quality of life and sustainable development at the state level, which is the basic form of organization of political communities today, it requires an adequate normative regulation in the number of areas, such as the protection of personal rights and transparency in the management process.

From that standpoint, the implementation of global networks and advanced information technologies contains challenges related to network security, protection of personality and democratic mechanisms, as well as the basic values of the state itself, *i.e.* national security. Facing these challenges involves mastering new dimensions of speed and quantity of information.

In the global network of networks of increasingly interconnected systems, people and things, we are faced with a growing number of sensors and users (especially through the IoT), including the number of points of entry into the system. This is why computer security becomes the value of interest for national security. Within this concept, the flow of information in its environment necessarily becomes dynamic and changeable [2], and thus, the perception in cyberspace is also becoming more challenging.

An additional challenge from the aspect of national security is due to the fact that in the space of decentralized communication, the state has no sovereignty over the Internet, in which that space exists.

2. THE CURRENT INHERENT CHALLENGES IN NATIONAL CYBERSPACE

In the first stage of internet communications, accessible content was static and there was a segregation of participants on creators and consumers of the contents. The second stage is characterized by overcoming of this division, in the sense that each user can simultaneously create and consume contents. Today, in the beginning of the third stage, the participants are becoming things (*e.g.* vehicles, kitchen appliances, lighting, medical equipment, buildings, clocks, nuclear reactors *etc.*), that can share information about itself and the environment on the network with other things or people. The capability of networked things is beyond the scope of computers and mobile phones and becomes the internet of interconnected things, which is finding an increasing application in healthcare, pharmaceutical industry, transport, energy, food industry, military industry, *etc.* From the technological aspect, the application of IoT enables qualitative changes, such as "personal robots", "smart homes and buildings," or other "smart" things, but also a better observation of global natural phenomena in meteorology, oceanography, geology, *etc.* In the research and commercialization of its results, vast resources are being invested by the largest actors in the market of information and communication technologies.[1]

Without the consent about the uniform code of communication (standardization) at the international level, IoT cannot realize the potential in implementation. Since there is an objective risk that standardization could be imposed by a dominant company or country [3], it represents a challenge in relation to the protection of rights of individuals and states.

Standards provide that different information systems can mutually exchange information. The most powerful participants, both commercial and national, attempt to impose their products or services as a de facto standard. But, they can simultaneously try to make them incompatible with products and services of other participants, thereby narrowing or disabling the choice [4]. In connection to this, the interoperability of the system also represents the protection against the dominant position and monopolistic behavior. Since, for example, the IoT is based on a number of different technologies and devices, whose capability and use are still not possible to hint from the aspect of national security, the challenge is also the standardization remains a challenge in certain areas. In this regard, the trust can be provided by the use of a transparent, open source code, and the regulation of the correct behavior of participants.

Many security issues of information systems on which the IoT is based might be relevant for individuals (*e.g.* electronic monitoring of patients) and for the states (*e.g.* monitoring critical infrastructures). A state, as one of the largest consumers and investors, can directly favor certain characteristics, and thereby improve transparency as well as the confidence and protection of personality [5]. The way in which the system of trust will be built depends on the legislator. The growing needs for data, rapid flow of information, the mass use of information and communication technologies require functional models of protection of privacy and personal data of citizens. Considering that many pieces of information of sensitive character are in circulation, IoT has the potential effect on the private and the public sphere.

1 Cisco - "Internet only", Ericsson - "Networked society", IBM -"Smarter Planet", Intel - "Intelligent systems", *etc.*

The systems for data collection and processing are designed to prevent the loss or damage of data and the period in which the devices monitor and store information is unlimited. Because of this, there is the risk of abuse of IoT in the field of surveillance in real time, in terms of interference in the private sphere of individuals or populations, and even in the physical integrity of citizens [6].

Limited availability also has the consequences in terms of individual cognitive processing, which are manifested in the form of tendency of users to, due to the benefits of constant availability, forget the information, and the need for constant suspicion [7]. Therefore, the application of technology, which by nature is not flexible enough and not learning from mistakes, should be regulated and functionally allocated to ensure the protection of personality.

Today's security methods are inadequate for the requirements of a vast system that the IoT should represent. The attacks, such as denial of service, unauthorized access, control over IoT device to insert corrupt information and manage the facilities, in contrast to the effects of the same attacks today, pose a risk to the entire system [8], and must, therefore, be anticipated before implementation.

3. THE VALUE NATURE OF CHALLENGES IN NATIONAL CYBERSPACE

Security, as a political value, is related to individual or societal value systems. As a concept, security is ambiguous and elastic in meaning. In an objective sense, it measures the absence of threats to acquired values, and in a subjective sense, the absence of fear that such values will be attacked. In international relations, security is conceived as an outcome of a process of social and political interaction, whose essential part are social values and norms, collective identities and cultural traditions, and from this perspective, it is necessarily intersubjective.

New uncertainties, however, introduce a challenge of a different type. Namely, they do not origin from individuals or social groups which can be prevented by the police and/or political measures, but rather from social risks, as a threat. This implies that security does not represent the situation without the (perception of) risk, but an ex-ante insurance, as a risk management technology, becomes the dispositions of social management. Diverting to insurance in the context of abstract risks results in security becoming the general social idea about value, and the universal normative concept, which is often used with different meanings.

In terms of security, threats, challenges, vulnerabilities and risks of a global network of networks require, on one side, a more precise defining, which would enable achieving a consensus on the new concepts and practical policy measures aimed at achieving agreed goals, and, on the other, a systematization of threats, challenges, vulnerabilities and risks of military, diplomatic, economic, social and environmental interests, as well as human security, food, health, energy and living conditions [9]. The perception of security in the application of nets network should include the value implications of control, data volumes, data access, data storage, the cost of security, data management, preferences for online presence and type of security staff and security checks [10].

Personal security, as one of the core values in the concept of national security, enjoys the protection in cyberspace, at the international level through two processes. First is the legal delegitimization of uncontrolled use of personal data, such as the prohibition of sending them to countries that do not provide adequate protection of privacy.[2] Publication of data on the Internet, however, is not considered as sending information to another country, although the approach is global, and they are available in the countries to which such information should not be sent. The second is related to the processing of personal data and protection of confidentiality of communications. Thus, for example, EU Member States are required to guarantee the confidentiality of communications by adopting national legislation which prohibits unauthorized interception, connecting, storing or otherwise intercepting communications, and individuals have the right to opt out of printed and electronic directories of telecommunications in relation to the processing of personal data and the protection of privacy in the telecommunications sector.[3] Concrete measures to reduce the obligations of operators to publish information regarding the use of personal data, including on how they will be treated, whether the site is monitored and the risks to privacy and data protection. These directives are not implemented when it comes to the interests of public security, defense or prosecution of crimes, which is the result of the compromise between the interests of protection of personal integrity and the need to provide an environment, prevent the commission of an offense,

2 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995.

3 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, Official Journal L 201, 31/07/2002

or catch the perpetrators. When, however, it's of concern of a potential threat to national security, countries are generally prone to interpret these restrictions are very narrowly.

In the upcoming phase of the information age, the issue of privacy protection is even more complex. The IoT, namely, unlike the communication between the users and the user and machine, involves much wider and more autonomous scope of communication between machines (such as the tag communication), which is why in the conditions of existence of the state, in addition to protection of the value system based on the human individual, it necessarily implies the national defining of standards that are of interest to the defense and security.

4. INFRASTRUCTURAL ASPECTS OF THE CHALLENGES OF IOT FOR NATIONAL SECURITY

The number of devices and sensors that could potentially fall within the IoT, from traffic control, health care, security to various levels of administration, grows even more in developing countries. In the extent that IoT implies, with the devices and equipment that are installed and produced by millions of producers, it seems impossible to provide security and due to that, the control and management and the security are the fields of IoT that require additional costs. The global annual cost of internet security breaches has by the beginning of the XXII century reached 115 billion dollars (Symantec, 2012). Sensitive applications, such as for the government, security services, and the finance, remain challenges for ensuring the security of supply. Functionally, *i.e.* in the field of mobility, IoT network represents a greater security risk from the point of the recipient than the transmitter, since security, encryption, and other services related to IPv6 do not have a major impact. It is a matter of ensuring the situation that the information that is directed in any direction leads to a reaction only of the user that is programmed to receive it. The first level of protection is a combination of markers and classification of the public categories. The only way to protect the terminals is by increasing the number of points to be controlled. A rational solution seems to be providing integration functions at the local level, as the devices themselves will have an access to a much wider range of devices [11].

The aim of classification and authorization of the receivers is to enable that the challenges concerning the network, relating to the separation of communication and access control near the terminal, are faced with in the three aspects of communication between machines: reaction in real time, deterministic performance and security. The point is that the systems in the cities use cameras and sensors for the safety and security purposes, and at the same time, in management, they have to meet the criteria concerning data privacy and security. Individual systems relating to control of the Cloud, in the cities (as well as in healthcare, energy, transportation, manufacturing, education), and consequently also to defining of groups, authorization and authentication, are mainly developed by companies.

As societies and networks become more complex and advanced, they become exposed to new risks and threats, and thus more vulnerable, national security, as well as public safety, become increasingly urgent requirements. In terms of the outreach, IoT may extend the range of business domains and value chains, including in the open environment [12]. What is emerging as a priority is the need to provide technological solutions for trust in the security of online networks. This requires anonymity of private data, but also the access of those in charge of national security and public safety.

In addition to trust, national security before the IoT infrastructure sets the requirements related to the rational decision making. IoT is already developing, and "smart" sensors and devices are collecting the statistics for mechanical decision-making and process, without actually being noticed, and the exponential growth is limiting human intuition and the expectations. Along with that, the computers are reducing in size so much that they are becoming things. Linking the physical world with the real world can not pass without consequences for the social organization, if for no other reason, then due to a higher available input of information and time consumption. This includes the basic components of decision making: data collection; data transmission and data analysis. It is impossible to evaluate whether the automatism of some decisions will enable the removal of heuristic, or if it only cause a bottleneck in the decision-making process. Concerning these potential developments, however, it is certain that the security aspect in general, and especially in relation to decision-making, is further compounded because of the risk due to greater opportunities for hacking and connectivity.

The interconnection in the network includes a number of security issues of the network itself: monitoring, control, collection of data, distributed control systems and other systems that perform the control function. Cybersecurity, and above all of the hacking, requires the standards, among which a key challenge is an access

to the content anytime and anywhere, especially in the application of Wi-Fi, which is a low level of protection [13]. The fact is that companies launch their security innovations, but it is debatable if they have an interest and scope to encompass all the challenges of IoT for national security since they have a primarily their own commercial interest.

Security passage ("smart" passages, like in health care or household protection) provides a point of entry into the network of the operator and that where the authentication is provided. Security, however, should also cover the manipulation with the data to be entered, such as certificates for passage that the operator issues, and which validates the entry. The problem is that this area users do not understand, and those functions must be provided in advance and automatically. Hence, security aspects such as confidentiality, integrity and authentication, must be included in the development phase of centralized solutions [14].

Public administration performs certain functions established by the law, including the national security. Some cyber systems have the potential to optimize the use of processing and storage, such as virtualization (running applications from the underlying hardware) and Cloud technologies (based on a virtualization), and allow the division between different administrative entities. From the standpoint of national security, the challenge is hosting authorities of the Clouds, which are beyond the institutional and democratic control.

Another problem is of legal nature, and it is concerned with the functional challenge that arises from omnipresent infrastructure environment (standards of openness and model data, hardware, computer power and network architecture) that IoT implies. Today, we are facing: new 'smart' systems currently available, new social media replacing old, Cloud computing, which is graded, flexible and everywhere; huge data sets, which are used in science, health, economy and everyday life. Secure and private Internet becomes a legal problem that is difficult to edit ex-post. The problem, from the aspect of national security, is the normative protection of values in relation to the interconnected networks, which could, according to some estimates, by 2040 be connecting in real time 50 to 100 trillion objects,[4] *i.e.* virtually everyone and everything. This will necessarily alter the basic norms of communication, which are today still anthropocentric, in a way that is difficult to anticipate.

Cloud goes beyond the current web system. Entities that operate autonomously perform tasks on behalf of other users or programs, and can thus modify the way of accomplishing the objectives. In the context of service-oriented network architecture, security challenge poses the fact that artificial intelligence enables solving some concrete problems, including the decision-making process, *i.e.* positions the physical and virtual entities that autonomously generate goals and objectives, which poses a risk to security and privacy in certain fields of application, especially relating to health.

5. THE CHALLENGES OF IOT FOR NATIONAL SECURITY IN A MATERIAL SENSE

In its specification, IPv6 includes security, such as encryption and authentication of sources in communication. However, when designing the architecture of interconnecting, and at the same time "smart", objects, specific challenges arise, such as networking between different technologies and domains, as well as the usability in terms of manageability, security, and privacy. In this regard, particular highlights are on the safety aspects of using sensors in chemistry, biology, radiology, and nuclear sector, in which context specialized bodies are formed to deal with network and information security at international level, like *European Network and Information Security Agency*). On the other side, surveillance system are being developed in large cities, like in London, where during 1990's a security monitoring system was introduced, called The Ring of Steel[5], or in New York, where in 2007 a plan was announced to install a system of antennas, radars, and roadblocks, in order to combat terrorists, named The Lower Manhattan Security).[6] From the aspect of value challenges of interconnectivity, the threats arise from the connection of "smart" data for the purpose of military control [15]. Due to the potential consequences of militarization of urban architecture, and in a broader sense also the fact that, because of flooding by applications, suppliers and stakeholders, existing standards are difficult to adjust, in order that the whole system is interoperable [16].

Interoperability is a special area of risk for safety, for themselves, for two reasons: firstly, because of the dissonance between the demands imposed by management and engineering, and, secondly, due to the perception

4 Becker, Albrecht; Sénéclauze, Grégoire; Purswani, Purshottam; Karekar, Sudharma; Internet of Things, Atos White Paper, 2013, p. 8. http://goo.gl/W29zDp (02.02.2016).

5 http://www.mascontext.com/issues/22-surveillance-summer-14/ring-of-steel/ (03.02.2016.)

6 http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml (03.02.2016.)

of decision makers and practical applicability of the developed forms do not provide a reliable solution. If security is viewed isolated, it seems to be contrary to the very idea of interoperability, which aspires to global inclusiveness and so equally globalized and challenges for the individual and national security of the states [17].

After Edward Snowden's revelations about the campaign of mass surveillance by the U.S. National Security Agency, the relation between cyberspace and human rights raises questions of national and international policies and the governance of the Internet, related to the resistance of sovereignty, the interests of national security and the shifting of the balance of power. Cyber espionage is a threat to national security because individual countries cannot respond to the global threat of terrorism, violation of human rights or environmental cooperation and coordination, even when they threaten international peace and security. In this sense, cyber defense entered the NATO strategy in 2002, and the cause were defensive operations in cyberspace against this organization during the illegal bombing of Yugoslavia in 1999 (especially through the state televison, RTS, whose building was bombed, even though it was a civilian object). This organization, as currently the only military alliance in the world, offers to the Member States and partner countries different mechanisms of "crisis management" and the help to strengthen national cyber defense capabilities. This way, it is introducing them into a uniform, practically collective mechanism of cyber defense of value concept on which the organization itself is based: freedom, common heritage and civilization of their peoples [18].

In the framework of the UN Security Council and other UN bodies, the issues of cyber security are only superficially addressed and, so far, there has been no indication that in the framework of international organizations working on an integrated and shared achievement of maintaining cyber security. Cyberspace is, in fact, often presented as a non-legal domain and conceptualized as an open, decentralized and participatory. However, the report of the UN Group of Governmental Experts confirms that international law, in the context of international security, in particular, the UN Charter, applies to cyberspace, and that the sovereignty and international rules and principles apply in relation to the behavior of the ICT and ICT infrastructure jurisdiction on the territory of the country.[7]

From the standpoint of national security, *ergo* in terms of the basic values, cyberspace can be perceived in two levels:

a) as a global domain within the information environment whose character is framed by the use of electronics and the electromagnetic spectrum, to create, store, modify, share and use information through independent, interconnected networks using information communication technology; [19] or

b) as an interconnected network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries[8], which is generally accepted to comprise the virtual environment and interaction between people.

One can observe three levels of cyberspace: physical (computers, integrated circuits, cables, communications infrastructure, *etc.*); software logic; and packs of data and electronics [20]. In that space, on one hand is a process of territorialization of cyberspace and cyber activity, in terms of territorial jurisdiction and powers, and on the other, deterritorialization, in terms of regulatory responsibilities from the extraction of certain territories.[9]

As the cyberspace permeates every aspect of modern society and is also the domain and the media through which the activities in the field of economy, public safety, civil society and national security are carried out.[10] The States have an interest that networks which support their national security and economic prosperity are secure and resilient. The reason for this is that the Internet can be used in a hostile interest at international level. As an examples of such use, the literature cites cases of massive and coordinated hacking in 2007 that stopped the economy and the administration of weeks in Estonia,

7 UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN doc. A/68/98 (24 June 2013), pp. 19-20.

8 National Security Presidential Directive 54, also Homeland Security Presidential Directive 23 (NSPD-54/HSPD 23).

9 Brolmann, Catherine, Deterritorializating International Law: Moving Away from the Divide between National and International Law, in: *New Perspectives on the Divide between National and International Law*, Nijman, Janne; Nollkaemper, Andre (eds.), Oxford: Oxford University Press, 2007, pp. 84-109. An example is the Internet Corporation for Assigned Names and Numbers (ICANN), which incorporated into the legal order of the United States, the contract with the Secretariat of the economy, but is independently responsible for keeping the Internet secure, stable and interoperable.

10 The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009. https://goo.gl/uUlxBx, 03.02.2016

and significant delay in development of Iran's nuclear program caused in 2009 by the infection with computer virus "Stuxnet" [21], as well as the action on the social networks with the aim to change the legal outcome of elections in Russia in 2011 [22].

Mass production of digital recordings creates opportunities for extensive public and private storage, processing, analysis, use and control, leading to initiatives to access and search for commercial, procedural and national security interests. The protection of privacy, cyber crime and espionage, make necessary protection of the Internet flow and reservoir digital records from unauthorized access and exploitation, even more complex. States, in many cases, restrict and censor content on the Internet, without any legal basis or on the basis of broad and vague regulations, without justification or need for that. In the field of expression the measures are applied, such as: blocking or filtering of content, including on social media sites; criminalization of political, social or religious content; imposing of liability for ISP that host or omit to block illegal content; disconnecting of users; cyber attacks on websites; monitoring of online activity; manipulation of online communications via commentators and spreading misinformation.[11] The legitimate purpose of these measures includes monitoring for prosecution, counterintelligence and national security while procedural requirements include a mandate in terms of the legal basis for surveillance, approval to conduct surveillance (*e.g.* a court order) and the necessity of control, or invasion of privacy proportional to the goal. The publicized revelations by Edward Snowden, in 2013, launched an issue of direct threats to civil rights, but at the same time, US President, Barak Obama, marked the cyber threats as "... one of the most serious challenges to national security".[12] In that sense, there is a need to protect confidential information and national infrastructure, primarily through the national security strategy, but also in relation to transnational threats for the common values of the international community [23].

11 UN Human rights council, *Report of the Repporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN dok A/HRC/17/27 (16 May 2011), para. 24; isto, Human Rights Committee, *General Comment 34 on Article 19: Freedom of Opinion and Expression*, UN dok. CCPR/C/GC/34 (12 September 2011) paras. 21-36.

12 Obama, Barrack, Taking the cyberattack threat serious, *Wall Street Journal*, 19.07.2012. http://goo.gl/U72pBx (03.02.2016); also, UK Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Presented to Parliament by the Prime Minister by Command of Her Majesty, October 2010. https://goo.gl/xFN61f (04.02.2016)

6. PROBLEMS IN THE APPROACH TO THE VALUE CHALLENGES IN CYBERSPACE

The original idea of communication between the devices was to meet the needs of the commercial exchange of information in real time. This has led to a situation where the communication in proximity can be misused for sharing content in an unauthorized spectrum. Ensuring that the end device can connect to the network, and the rest are disabled, has imposed the need to define national standards for interoperability in the field of security. It seems that aute problems of information security must be addressed in local networks [24].

Trends in access, availability, speed and recursive simplicity have implications on the relations between people in terms of the empowering of individuals and the organization of public dimension. Expanding of the range of participants and situations that have the capacity, in terms of interconnections in cyberspace, to compromise the value system of societies, without necessarily military threats. The organization of national security, with the primary aim to prevent distortion or destruction of basic national values and property, implies a multidimensional conflict and defense. Governments alone can not ensure national cyberspace, but they are responsible for it. This leads to problems of where the line of defense stops, the limiting of participants, or expanding the security model (such as preventive attacks, which has led to the spread of covert operations and military actions against state information systems) [25]. Today, the emphasis is on public diplomacy, as a tool of national security (especially on social networks).

The changes that interconnection brings in the concept of conflict, the role of government participants, the doctrine of preemptive action, the relationship between high-tech versus low-technology, have led to changes in the concept of the Internet, in terms of involvement of fields of possible abuses and distortions. National security includes the decision-making process, which now involves a problem of perception and human capacity to capture details; as well as the power, which is now going through a phase of reformulation and redistribution, as soft and smart power and involves research centers and companies [26], but also redefining foreign policy objectives, in terms of restrictions, privacy and access.

7. CONCLUSIONS

The number of participants, information, and potentially objects, intensity, quantity and rate of exchange, in cyberspace, make it impossible to reliably and accurately

determine the potential value challenges that countries will face in the efforts to preserve their fundamental values, *i.e.* their national security. This is especially emphasized in the new historical situation, in which the process of globalization is taking place alongside with the digitalization.

In order to face the anticipated risks, the executive branch necessarily has to establish the control over the risky sectors, with which citizens, the economy, public administration, as well as all students who violate the fundamental values of society, come into contact.[13] At the broadest level, the responsibility of the state to its citizens imposes the necessity of establishing a national strategy in the field of information development, on the basis of which it would be possible to establish norms in the national cyberspace in order to protect the fundamental values of the community.

Adjusting the current and the future needs and challenges of interconnected cyberspace requires training of individuals. On one hand, through the educational system, in order to value the education of personality capable of rational perception of content in cyberspace.[14] On the other hand, it also includes professional training of users at all level, of public administration for safe participation in cyberspace.

In addition to planning and training on the national level, it is necessary to ensure the protection of infrastructure and personalities, including legal regulation of the parameters before the application of new technologies, since due to the extreme global inclusiveness, cyberspace is almost impossible to regulate subsequently, without prejudice to the interconnected participants.

REFERENCE

[1] RFID Working Group of the European Technology Platform on Smart Systems Integration, *Internet of Things in 2020: Roadmap for the Future*, Brussels: European Commission, 2008, p. 6; Tommasetti, Aurelio; Vesci, Massimiliano; Troisi, Orlando, The Internet of Things and Value Co-creation in a Service-Dominant Logic Perspective, in: *Data Management in Pervasive Systems*, Colace, Francesco *et al.* (eds.), Springer, 2015, p. 6.

[2] Minoli, Daniel, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, New Jersey: Wiley, 2013, p. 63.

[3] Riillo, Cesare, Profiles and Motivations of Standardization Players, in: *Standards and Standardization: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications Management Association*, Information Resources Management Association (ed.), Hershey: IGI Global, 2015, pp. 987-988.

[4] Kim, Sangbae; Hart, Jeffrey, The Global Political Economy of Wintelism: A New Mode of Power and Governance in the Global Computer Industry, in: *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, Rosenau, James; Singh, N. J. P. (eds.), New York: State University of New York Press, 2002. pp. 149-154.

[5] Kummer, Markus; Seidler, Nicolas, Internet and Human Rights: The Challenge of Empowered Communities, in: *Human Rights and Internet Governance - MIND 4*, Kleinwächter, Wolfgang (ed.), Berlin/Baku: Internet & Gesellschaft Collaboratory, 2012, p. 53.

[6] Bibri, Simon Elias, *The Shaping of Ambient Intelligence and the Internet of Things: Historico-epistemic, Socio-cultural, Politico-institutional and Eco-environmental Dimensions*, Amsterdam: Atlantis Press, 2015, p. 221.

[7] Lagemaat, Richard van de, Theory of Knowledge for the IB Diploma, 2nd Edition, Cambridge: Cambridge University Press, 2015, p. 266.

[8] Dhanjani, Nitesh, *Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts*, Sebastopol CA: O'Reilly, p. 231-234.

[9] Brauch, Hans Günter, Concepts of Security Threats, Challenges, Vulnerabilities and Risks, in: *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks*, Brauch, H.G. *et al.* (eds.), Berlin/Heidelberg: Springer, 2011, p. 105.

[10] Patil, Sunil *et al.*, *Public Perception of Security and Privacy: Results of the comprehensive analysis of PACT's pan-European Survey*, Santa Monica: Rand Corporation, 2015, pp. 33-34.

[11] Costa, Francis da, *Rethinking the Internet of Things: A Scalable Approach to Connecting Everything*, New York: Apress, 2013, p. 158.

[12] Holler, Jan *et al.*, *From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence*, Oxford/Waltham: Academic Press, 2014, p. 66.

[13] Behmann, Fawzi; Wu, Kwok, *Collaborative Internet of Things (C-IoT): For Future Smart Connected Life and Business*, London/New Jersey: John Wiley & Sons, 2015, p. 128.

13 In: Đurđević, Dragan; Stevanović, Miroslav, „Problems Faced By IT Sector in Serbia in Combating Money Laundering", *FBIM Transactions* 3:1/2015, p. 185.

14 Stevanović, Miroslav; Đurđević, Dragan, *The Capacity of Perception: The Need for an Educational System in Support of the National Security*, The Fourth International Scientific Conference "Employment, Education and Enterpreneurship", 14-16 October 2015, Belgrade, Proceedings, 2015, p. 55.

[14] Rita, Maria *et al.*, 6TiSCH Wireless Industrial Networks: Determinism Meets IPv6, in: *Internet of Things: Challenges and Opportunities*, Mukhopadhyay, Subhas Chandra (ed.), Dordecht: Springer Science & Business Media, 2014, p. 129; also: Fazio, Maria *et al.*, An Integrated System for Advanced Multi-risk Management, in: *Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful*, Gaglio, Salvatore; Lo Re, Giuseppe (ed.), Dordecht: Springer Science & Business Media, 2013, p. 261.

[15] Ovidiu, Vermesan *et al.*, *Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains, Ecosystems and Market*, Vermesan, Ovidiu; Friess, Peter (eds.), Aalborg: River Publishers, 2015, p. 80.

[16] Minoli, Daniel, *Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications*, London/New Jersey: John Wiley & Sons, 2013, p. 103.

[17] Waher, Peter, *Learning Internet of Things*, Birmingham/Mumbai: Packt Publishing, 2015, p. 214.

[18] Ziolkowski, Katherina, NATO and Cyber Defence, in: *Research Handbook on International Law and Cyberspace*, Tsagourias, Nicholas; Buchan, Russell (eds.), heltenham/Northampton: Edward Elgar Publishing, 2015, p. 427.

[19] Kuehl, Daniel, From Cyberspace to Syberpower: Defining the Problem, in: *Cyberpower and National Security*, Kramar, Franklin; Starr, Stuart; Wentz, Larry (eds.), National Defence University Press, 2009, p. 28.

[20] Tobanksy, Lior, Basic Concepts in Cyber Warfare, *Military and Strategic Affairs*, 3:1/2011, pp. 77-78.

[21] Buchan, Russell, Cyber Attacks: Unlawfull Uses of Force or Prohibited Interventions?, *Journal of Conflict and Security Law*, 17:2/2012, pp. 218-221.

[22] Stevanović M. D., Đurđević D. Ž. (2015), *National Security Challenges in Cyberspace of Social Networks: Case Study "Navalni"*, Proceedings, ISBN 978-56-86745-56-9. Scientific Expert Conference: Forensic Audit 2015, Belgrade, 10-11. Decembar 2015.

[23] Buchan, Russell, Cyber Espionage in International Law, in: *Research Handbook on International Law and Cyberspace*, Tsagourias, Nicholas; Buchan, Russell (eds.), heltenham/Northampton: Edward Elgar Publishing, 2015, p. 179.

[24] Masek, Pavel; Muthanna, Ammar; Hosek, Jiri, Suitability of MANET Routing Protocols for the Next-generation National Security and Public Safety Systems, in: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, 15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART 2015, St. Petersburg, Russia, August 26-28, 2015, Proceedings, Balandin, Sergey; Andreev, Sergey; Koucheryavy, Yevgeni (eds.), Dordecht: Springer, 2015, pp. 244-245

[25] Harknett, Richard, Integrated Security: A Strategic Response to Anonymity and the Problem of the Few, in: *National Security in the Information Age*, Goldman, Emily (ed.), New York: Routledge, 2004, p. 150.

[26] Hart, Jeffrey, Information and Communications Technologies and Power, in: *Cyberspaces and Global Affairs*, Perry, Jake; Costigan, Sean (eds.) Aldershot/Burlington: Ashgate Publishing, 2013, pp. 206-207.