Information & Security: An International Journal

Baraković & Baraković Husić, vol.32, 2015 http://dx.doi.org/10.11610/isij.3205

"WE HAVE PROBLEMS FOR SOLUTIONS": THE STATE OF CYBERSECURITY IN BOSNIA AND HERZEGOVINA

Sabina Baraković and Jasmina Baraković Husić

Abstract: The Internet and information communication technologies (ICT) became the most important components in everyday life, given the fact that they have altered the behaviour patterns and in many aspects made our lives simpler. Upcoming Internet of Things (IoT) will additionally have a positive influence on our Quality of Life (QoL). However, even now, the society is extremely vulnerable to disturbances that may affect the functioning of the Internet and ICT systems, and thereby jeopardise the reliability and security of the information they contain. The situation becomes even more complicated when IoT takes effect and cyber threats exceed the perimeter of information security and include physical security, existence and health. The world has shyly started to raise questions and perceive problems regarding the IoT, QoL and security issues that it will bring to the cyber space in order to find the appropriate solutions in time. Bosnia and Herzegovina, as well as any other modern country, needs to take place in these processes and newly opened research fields. This paper gives an overview of Bosnia and Herzegovina's existing cybersecurity infrastructure and capacities in terms of legislation, security management structure, corresponding cybersecurity units, as well as their cooperation and qualification level. On that basis it is concluded that cybersecurity is not among the priorities in Bosnia and Herzegovina. The country "offers" problems for adequate and generally accepted solutions in the cybersecurity domain and needs to work on its readiness to contribute to the safety of IoT and cyber space, and consequently improving citizens' QoL.

Keywords: Bosnia and Herzegovina, cybersecurity, Internet of Things, cybersecurity legislation, cybersecurity units, cybersecurity cooperation.

Introduction

Throughout the last decades the Internet, communication networks and information systems have experienced a phenomenal growth and thereby completely changed the lives of most people as well as the ways in which they communicate, obtain and exchange information, entertain, do business, take care of their health and environment, learn, govern, etc. Simultaneously, the rapid development of wireless mobile commu-

nications has increased users' requirements and expectations in terms of accessing a wide variety of services, i.e., anywhere, anytime, and via multiple devices.[1] Being relied on in everyday life has made the information communication technologies (ICT) one of the most important component of peoples' Quality of Experience (QoE) and consequently the Quality of Life (QoL), since it has altered the behaviour patterns and in many aspects made our lives simpler.

However, this rapid technological change which has resulted in many aspects of our lives being connected and affected by digital communications is just an introduction phase for what is about to take place – the Internet of Things (IoT). The IoT is the network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment.[2] Although IoT is a hot topic nowadays, it is not a new concept. The phrase was coined by Kevin Ashton in 1999: "If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."[3] The IoT will help to enable an environment with the flexibility to provide services of all sorts, ranging from home automation to smart retail/logistics, and from smart environmental monitoring to smart city services. It will enable sensing, analytics and visualisation tools, which will be accessed by anyone, anytime and anywhere in the world on personal, community or a national level.[4] Many opportunities that IoT will offer, such as creating new business opportunities (e.g., IoT data enabling organisations to better understand customers' requirements), improving decision making (e.g., real-time updates, enhances facilities, more accurate fact finding will lead to more informed decision-making), reducing costs (e.g., IoT-linked devices will get more affordable in case of failure), improving safety and security, improving users' experience and lives (e.g., ease of access, ease of living, ease of communicating), improving infrastructure, etc., will result in key sectors such as health care, education, financial, retail, communications, hospitality, industry and agriculture benefiting from IoT. In other words, peoples' QoL will benefit from IoT.

On the other hand, given that even today the majority of records and processes containing information have been computerised and automated, the society has already become extremely vulnerable to disturbances that may affect the functioning of ICT systems and the Internet, and thereby jeopardise the reliability and security of the information they contain.[5] The situation tends to become even more complicated when IoT takes effect and threats exceed the perimeter of information security and include physical security, existence and health. While IoT is entering daily life more and more, security risks pertaining to it are growing and changing rapidly. In future "al-

ways on" and "all connected" technology environment amplified with users' low security awareness, attacks and threats in cyber space are just a matter of time. In other words, besides the advantages that IoT provides, it also introduces many issues.

Namely, the IoT can be perceived as the medium of interconnection for people, and since human communication is mediated by machines and becomes more indirect, there is a deeply rooted security problem with the possibility of impersonation, identity theft, hacking, and in general cyber threats. Further, the IoT will increasingly rely on cloud infrastructure which in general lacks security and great number of smart devices, ranging from garment to house furniture or vehicles, with a vast number of applications to support them, thus introducing challenges to data privacy, data protection, safety, governance and trust. Security matters in the IoT products of today and tomorrow.

If security is not addressed in the IoT, there is a very real risk that instead of benefiting from the gains in security witnessed in desktop and mobile computing, we will instead regress, creating a larger attack surface of devices that are more vulnerable or provide ways into larger systems. This presents a very real risk – if security is not taken seriously by regulators, legislators, and markets, we will instead be in a worse situation than we are today.[6]

Further, today people value quality, and their experiences, perceptions and needs with respect to a particular product, service or application are of greater importance.[7] That is the reason for an intense user-oriented approach in various fields aimed at improving quality of human life, which refers to IoT as well. On the other hand, activities aimed at compromising the IoT cyber space and threats against it are rising and may have increasingly serious consequences for individuals, business, private and public institutions, as well as society in general, since they could disrupt the supply of essential services taken for granted, such as water, electricity, mobile services, etc. The question that rises from above presented facts, i.e., new opportunities and benefits that peoples' QoE and QoL will experience from IoT on one side and cybersecurity risks that IoT brings with itself on the other, is how to effectively model and balance the presence of IoT? In other words, one must find the threshold where the IoT's contribution to quality of experience and life must be neglected and security in cyber space given a priority, and vice versa. Where is the balance? What kind of model should it represent? Is it going to be individually based or a general model? One needs to start answering all these (and many more upcoming) questions and solve related issues now in order to successfully manage and maximise the usage of IoT and minimise the security problems that arise within cyber space, since in the near future problems will get even more complex. In other words, we must manage the IoT before it starts managing us.

When it comes to QoL, people in Bosnia and Herzegovina have the same opportunities and requirements in terms of new technologies as anywhere else in Europe or the modern world. However, the awareness on cyber threats in IoT in countries, institutions, organisations and of individuals in the modern world is on a much higher level than in Bosnia and Herzegovina. Advanced societies have harmonised the legislation and established and strengthened specialised units for enhancing the capacity to provide cybersecurity. Bosnia and Herzegovina has unfortunately done very little in this field due to many specific and complex issues, discussed in this paper, ranging from security management organisation to legislation and security units to lack of cooperation and low levels of qualification. Therefore, the majority of offered, possible and adequate cybersecurity solutions applied in countries worldwide in terms of legislation, specialised units, organisations, etc., experience difficulties and are practically inapplicable in environments such as this country. Also, ensuring cybersecurity in Bosnia and Herzegovina is a challenging task due to a mentality dominated by the issue of who is going to be in charge (the boss), instead of perceiving the broader picture and acting for the "global" benefit. Ensuring cybersecurity, however, requires unselfish, nonexclusive and joint act of all stakeholders for the purpose of free, efficient and safe use by people of cyber space, the Internet and future IoT.

This paper provides an overview of general cybersecurity in Bosnia and Herzegovina given that cyber space knows no boundaries in traditional context and weaknesses in this country may have an impact anywhere in the world. Therefore, the paper addresses the most common cybersecurity incidents in this country, issues related to the security management structure, legislation and terrorism, cybersecurity units and their internal and international cooperation, as well as the level of qualification.

Cybersecurity Incidents in Bosnia and Herzegovina

Bosnia and Herzegovina's police agencies officially have not recorded advanced technology cyber incidents (related to IoT), but it is a matter of time when they will occur. However, hitherto cybersecurity incidents in Bosnia and Herzegovina included cyber crime and terrorism activities in which crimes or offenses include computer devices (computers, laptops, mobile phones, smartphones, tablets, etc.) and networks, and computer data as objects or means of illegal activity. The examples of cyber criminal activities in Bosnia and Herzegovina can be summarised in the following points:[8]

- DoS (Denial of Service) and DDoS (Distributed DoS) attacks – mostly directed against websites of private companies for the purpose of extortion;
- Internet fraud – including fraudulent lotteries, where the citizens of Bosnia Herzegovina were the victims;

- Unauthorised access to computer systems and networks by cracking user identities (IDs) and passwords or by other illegal means of obtaining those codes; when having obtained access directly affecting the final outcome of electronic data processing thereby damaging legal entities in Bosnia and Herzegovina;
- Credit cards scams – by means of skimming and phishing;
- Phishing and vishing attacks;
- Wireless network abuse – using the appropriate software programmes criminals illegally used "wireless" network without payment thereby inflicting a monetary damage to the Internet Service Providers (ISPs);
- Child pornography on the Internet – police discovered a large number of offenders committing abuse of children on the Internet;
- Intellectual property rights violation on the Internet – unauthorised access, distribution, and possession of video, audio, books, papers, etc. protected by intellectual property rights;
- Social networks abuse – identity theft, extortion, online mistreatment, etc.;
- Distribution of malware;
- Inciting national, racial, and religious hatred, discord, or intolerance on websites, blogs, forums, social networks, etc.;
- Public incitement to terrorism and terrorist propaganda on websites, blogs, forums, social networks, etc.

Security Management Structure Issues in Bosnia and Herzegovina

Security management structure in Bosnia and Herzegovina is extremely complex and in line with the country's complex organisation. Namely, Bosnia and Herzegovina is divided in two entities: Federation of Bosnia and Herzegovina, which consists of 10 cantons, Republic of Srpska; and Brčko District (Figure 1). Taking this fact into consideration, multiple security bodies and police agencies exist and operate on the territory of Bosnia and Herzegovina, but on different state level, i.e., the state, entity or canton level.

Bosnia and Herzegovina has several security management bodies on the state level. First, there is the Ministry of Security of Bosnia and Herzegovina.[9] The competences of this institution are not defined in the Constitution of Bosnia and Herzegovina,[10] but within the Law on ministries and other administrative bodies in Bosnia and Herzegovina.[11]

The Ministry of Security of Bosnia and Herzegovina includes several police bodies as its administrative constituent parts: Directorate for Coordination of Police Bodies of

Bosnia and Herzegovina,[12] Border Police of Bosnia and Herzegovina,[13] State Investigation and Protection Agency,[14] Forensic Examination and Expertise Agency,[15] Personnel Education and Professional Development Agency,[16] Police Support Agency,[17] and Service for Foreigners' Affairs.[18] All listed agencies have the corresponding competences in terms of ensuring the security on the state level.

Further on, in addition to abovementioned organisations for state level security management, a number of them exist on lower levels of government. On the entity level there are the Federal Police Administration[19] and Ministry of Interior of Republic of Srpska.[20] In the Federation of Bosnia and Herzegovina, due to existence of 10 cantons, security issues are in the competence of 10 corresponding ministries of internal affairs in: Una-Sana Canton, Posavina Canton, Tuzla Canton, Zenica-Doboj Canton, Bosnian Podrinje Canton, Central Bosnia Canton, Herzegovina-Neretva Canton, West Herzegovina Canton, Sarajevo Canton, and Canton 10. Additionally, Police of Brčko District[21] operates on the territory of Brčko District. Each of these institutions has operational competence on the corresponding territorial unit in Bosnia and Herzegovina.

With this complex and decentralised structure of the country and security management it is extremely challenging and slow to perform activities or achieve consensus in this sector. Who should then be in charge of cyber risk management? Having too many silos, i.e., security organisations, leads to too many bad decisions, since each of them is thinking about its world. Too many bad decisions lead to too much complexity, while in the end too much complexity leads to risk. Therefore, attempts to apply traditional security approaches and solutions to combat cyber crime or terrorism and improve cybersecurity in environments such as Bosnia and Herzegovina often fail. Moreover, activities such as initiation of strategic activities, decision making, taking over responsibility, and many others that would benefit the country and its citizens are additionally complicated by collision caused by the opposite political stances and goals in Bosnia and Herzegovina. The leaders in Bosnia and Herzegovina pay insufficient attention to cybersecurity. Cybersecurity requires a different approach that implies equality, openness and trust among interested parties and acts aimed at gaining the general benefit. In the end, alternatives are needed, not vetoes. However, the current situation implies that until something bad in cyber space happens to someone important in the country no major steps will be made.

Cybersecurity Related Legislation Issues in Bosnia and Herzegovina

Bosnia and Herzegovina has signed international agreements and conventions relevant to information and cybersecurity. The most prominent ones are the Convention

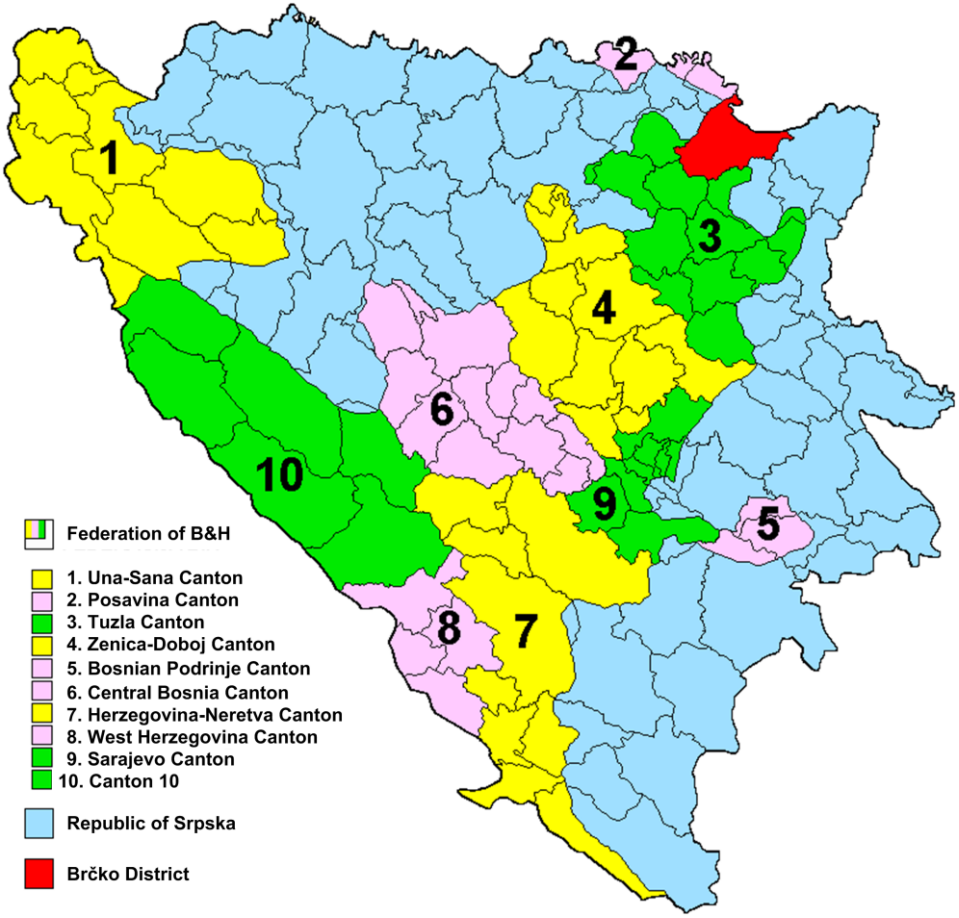

Figure 1: The territorial organisation of Bosnia and Herzegovina.[22]

on Cybercrime[23] and the Stabilisation and Association Agreement.[24] The Convention has been signed on 23 November 2001 in Budapest, while the Presidency of Bosnia and Herzegovina has reached the decision on ratifying the document at its 89th session held on 25 March 2006.[25] Thereby, Bosnia and Herzegovina obliged to adopt legislation and other necessary measures for combating cybercrime in order to harmonise them with other signatories of the Convention in terms of felony treatment, data acquisition, processing and storage.

For its part, the Agreement specifies 25 cooperation policies, where the most important articles in the area of information and cybersecurity are the ones defined by Article 103 on "Information society," Article 104 on "Electronic communication

networks and services," and Article 105 on "Information and communication." By signing it on 16 June 2008 in Luxembourg, Bosnia and Herzegovina undertook the obligation to align its legislation regarding the information and cybersecurity, and to establish implementation mechanisms.

However, Bosnia and Herzegovina has not adequately progressed in the cybersecurity field, nor has it harmonised its legislation accordingly. Namely, just as it is the case with the security management structure in Bosnia and Herzegovina (presented in the previous section), the legislation in the country reflects the complex and decentralised organisation of the country.

The existing legislation on the state level that may be related to cybersecurity only scarcely and partially addresses relevant issues and has not fully implemented the regulations provided by the Convention on Cybercrime (Table 1). The Ministry of Communications and Transport of Bosnia and Herzegovina initiated the drafting of amendments on the existing Law on Communications and it is expected that certain issues in this area will be regulated in a more effective manner.[26]

In addition, the Ministry of Security of Bosnia and Herzegovina has passed several documents that address cybersecurity: the Strategy for Establishment of BIH CERT[27] – the first document on the state level that addresses cybersecurity directly, the Strategic Plan of the Ministry of Security 2016-2018, the Strategy for Combating Organized Crime 2014-2016,[28] Memoranda of Cooperation and Mutual Assistance between the Ministry of Security of Bosnia and Herzegovina and the Association for Protection of Audiovisual Works in Bosnia and Herzegovina,[29] Action Plan for Protection of Children and Prevention of Violence over Children via Information Communication Technologies in Bosnia and Herzegovina 2014-2015,[30] Agreement between the Ministry of Security of Bosnia and Herzegovina and Europe Police College (CEPOL) on Training Police Officers in Accordance with European Standards,[31] and Decision on Legal Interception.[32]

Further on, taking a top-down approach in terms of country organisation, Table 2 contains a comparison of regulations of the criminal legislation of entities and Brčko District,[33] which have partially implemented the recommendations of the Convention on Cybercrime (Articles 2 to 9). These issues are not addressed in the Criminal Law of Bosnia and Herzegovina[34] since they have been conceded by agreement to the criminal legislation on the entity levels (and Brčko District). In addition, cybersecurity issues have been addressed in the Criminal Procedural Law of entities and Brčko District[35] and the Law on Electronic Signature, Law on Electronic Document, Law on Electronic Management in Republic of Srpska.[36] Also, Republic of Srpska has adopted the Law on Information Security[37] which defines information security that is being ensured by applying measures and standards of information security, addresses

protection of data in the government of this entity, and determines bodies for adaptation, implementation and monitoring of subject measures.

Table 1: State level legislation related to cybersecurity.

Law	*Implementation*	*Article*
Criminal Law[38]	Criminal offenses related to violation of copyright (Implemented)	242, 243, 244, 245, 246
	Incitement of national, racial, and religion hatred, discord, and intolerance (Partially implemented)	145
	Corporate liability (Implemented)	122
	Attempt and aiding or abetting (Implemented)	29, 30, 31
Criminal Procedural Law[39]	Definitions (Partially implemented)	20
	Production order (Implemented)	72a
	Search and seizure of stored computer data (Implemented)	51
	Surveillance and technical recording of telecommunications (Partially implemented)	116
Law on the Protection of Personal Data[40]	Data security (Partially implemented)	11
Law on the Protection of Classified Data[41]	Protection of classified data (Partially implemented)	77
Law on Communications[42]	Data security (Partially implemented)	5, 15
Law on Electronic Signature[43]	Fully implemented	
Law on Electronic Legal and Business Transactions[44]	Fully implemented	
Law on Prevention of Money Laundering and Financing of Terrorism[45]	Partially implemented	26

The scarcity and disharmony of legal regulations in the field of cybersecurity in Bosnia and Herzegovina indicates that there is a need for systematic approach from the government at the state level in treating these matters. However, each attempt to update and harmonise the legislation encounters the same issues as those present in security management section – the lack of political awareness and will. Each postponement of new adoptions and harmonisation additionally complicates the situation, distorts the application of European Union (EU) recommendations, supports the technology lag of the country and exposes all information systems in Bosnia and Herzegovina to greater security risks. In addition, since one of the main foreign policy ob-

jectives of Bosnia and Herzegovina is the full EU membership, Bosnia and Herzegovina will inevitably have to adopt new and harmonise its current legislation regarding cybersecurity in line with the EU's, and reorganise existing or establish corresponding bodies for the enforcement of the subject legislation. Specifically, this refers to the requirements of recently published Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[46] and the proposed Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union[47] that is about to be adopted on the EU level.[48]

Table 2: Comparison of regulations of criminal laws that have implemented the recommendations stipulated by the Convention on Cybercrime on the entity level and Brčko District.[49]

Offense	*Article of FBIH CL*	*Article of RS CL*	*Article of BD CL*
Damaging computer data and programs	393	292a	387
Computer sabotage	392	292b	392
Development and entry of computer viruses	-	292v	-
Computer fraud	389	292g	389
Unauthorized access to protected computer, computer network, telecommunication network and electronic data processing	391	292d	391
Prevention and restriction of the access to public computer network	-	292đ	-
Unauthorized use of computers and computer network	-	292e	-
Computer adulteration	388	-	388
Obstruction of the system and electronic data processing network	390	-	390
Unauthorized optical recording (photography)	189	175	186
Usage of the child or minor for pornography	211	199	208
Introducing a child to pornography	212	-	209
Producing and presentation of child pornography	-	200	-

Legend: BD (Brčko District), CL (Criminal Law), FBIH (Federation of Bosnia and Herzegovina), RS (Republic of Srpska).

Cyber Terrorism Related Issues in Bosnia and Herzegovina

As the rest of the world, Bosnia and Herzegovina deals with issues and challenges related to public incitement to terrorism and terrorist propaganda together with national, racial, and religious hatred, discord, or intolerance in cyber space, i.e., on

websites, blogs, forums, social networks, etc. Some of the challenges are a projection of the world trends, while others appear as a consequence of the aggression on Bosnia and Herzegovina in the 1990's. In dealing with the subject offenses, Bosnia and Herzegovina refers to Article 201 on "Terrorism" and Article 202 on "Financing of Terrorist Activities" of the Criminal Law in Bosnia and Herzegovina.[50] In addition, the Ministry of Security of Bosnia and Herzegovina has started working on the draft of the Strategy on Combating Terrorism 2015-2020, which will address cyber terrorism issues in Bosnia and Herzegovina in detail.

Cybersecurity Units in Bosnia and Herzegovina

Advanced European countries have raised awareness regarding cyber issues, since their citizens require trust and confidence when conducting various activities online. Consequently, their governments have not only harmonised legislation, but also established and strengthened specialised units for enhancing the cybersecurity accordingly. On the other hand, Bosnia and Herzegovina has made quite small steps in this field. Hereof and due to the low cybersecurity awareness, together with the complex security management organisation on its territory (country's specific organisation and multiple police agencies) and technological lag in comparison to advanced European countries, Bosnia and Herzegovina is more susceptible to risks and threats in the cybersecurity domain.

Motivated by the serious repercussions for individuals, business and society, that the cyber threats could cause, and additionally motivated by EU recommendations on the formation of cybersecurity bodies in all member countries and potential member countries, the Ministry of Security of Bosnia and Herzegovina in accordance with its governmental competences proposed the previously mentioned *Strategy for Establishment of CERT in Bosnia and Herzegovina* (hereinafter: The Strategy).[51] With the Strategy, the formation of Computer Emergency Response Team (CERT) in Bosnia and Herzegovina – BIH CERT – has been initiated. The Strategy was adopted by the Council of Ministers at its 156th session held on 28 July 2011, thereby, as already noted, becoming the first document at the state level dealing concretely with cybersecurity issues.

The Strategy provided for formation of the Working Group for the establishment of CERT in Bosnia and Herzegovina. The Ministry of Security of Bosnia and Herzegovina submitted a draft Decision on establishing and appointing an Expert Working Group which was formed by the Council of Ministers at its 168th session held on 7 December.[52] During its mandate, the Working Group established connections with relevant international organisations, such as the North Atlantic Treaty Organization (NATO) and the Organisation for Security and Cooperation in Europe (OSCE). Authorised to represent Bosnia and Herzegovina in CERT matters, it connected with

other CERTs in Europe, the European Union Agency for Network and Information Security (ENISA), the Task Force Collaboration Security Incident Response Teams (TF-CSIRT), etc. In addition, its members made study visits to other countries to collect information on their experiences. Importantly, it drafted an Action Plan[53] which is still pending adoption by Council of Ministers.

Although the Strategy, the Working Group or the formation of a preventive body such as BIH CERT will not resolve all cybersecurity issues in Bosnia and Herzegovina, these are important steps in the implementation of a systematic approach of building the fundament of the overall government strategy by legislation, i.e., assuring and improving the cybersecurity in the country by adopting new legislation or harmonising existing one in this field.[54]

BIH CERT has been envisioned as a preventive body that gives recommendations for the application and improvement of security measures for protecting information systems of Bosnia and Herzegovina's government institutions. Hence, BIH CERT should not include operational problem solving. Although it is not yet established, the vision of BIH CERT should be based on the fulfilment of several assumptions:

- BIH CERT should achieve adequate coordination and cooperation between the relevant bodies in Bosnia and Herzegovina;
- The scope of cooperation should be expanded into the fields of industry, education and development, through coordination with the manufacturing companies, higher education institutions and research centres;
- The activity of BIH CERT should be expanded outside the borders of Bosnia and Herzegovina by cooperating with international CERTs, organisations such as ENISA and TF-CSIR and international computer manufacturing companies (hardware and software), all for the purpose of mitigating or eliminating the consequences of security emergencies.

Further on, the mission of BIH CERT should be to continuously increase the reliability of critical infrastructure, work on prevention and minimisation of possibilities for security emergencies, provide assistance to the administrators of critical infrastructures in applying proactive measures for risk reduction and in reducing the consequences of security emergencies.

BIH CERT should perform both proactive and reactive activities. In a proactive sense, BIH CERT should act before an emergency or another event that may endanger the security of the information systems, for the purpose of preventing or mitigating possible damage. Among the proactive measures are: (i) providing security warnings; (ii) monitoring ICT security technologies; (iii) disseminating information from the field of ICT security; (iv) promoting awareness of the importance of ICT se-

curity; and (v) offering ICT security education and training. In addition, proactive measures should be published. On the other hand, reactive activities should include support in processing ICT security emergencies in several aspects, such as: (i) determination of an emergency, which includes determination of whether an observed event could be classified as an ICT security emergency and the scope of the emergency, together with development and distribution of security warnings; (ii) coordination of emergency solutions, which includes cooperation and coordination with CERTs or other relevant bodies in Bosnia and Herzegovina; and (iii) provision of emergency solutions, including security warnings and coordination in solving emergencies.[55]

Further on, when it comes to elaboration of short-, mid-, and long-term strategic goals, BIH CERT should immediately, upon its establishment, submit a request for registration/accreditation by the relevant international institutions and establish direct communication and cooperation with ENISA, TF-CSIRT, national CERTs from the region as well as the most significant CERTs in Europe and globally. Also, BIH CERT should identify critical infrastructure in Bosnia and Herzegovina that needs protection and establish contacts and define rules for information exchange with the administrators of such infrastructure. Besides its advisory role, another goal of BIH CERT is education. In that context, BIH CERT should publish bulletins with the latest information regarding security and proactive measures for risk reduction on a continuous basis. Education also includes the organisation of regular workshops for security administrators of critical infrastructures. With the realisation of its mid-term goals, BIH CERT should identify other information systems which require assistance on security issues and expand its activities towards them. This, together with the continuous evaluation of the security state of the critical infrastructure and critical infrastructure administrators' education, will improve the general state of security. The long-term goal is to support the establishment of CERTs on different state levels as well as ones in private and academic sectors.[56]

There are two models based on which the BIH CERT body could be established:[57]

- Model 1: BIH CERT as an independent administrative organisation or a special body of the corresponding ministry;
- Model 2: BIH CERT as a constituent of the corresponding ministry.

The first model would require the adoption of a state law on BIH CERT that would arrange all aspects of BIH CERT's functioning, beginning with the establishment, mandate, financing, competences, organisation and management. However, the EU practice is not to adopt regulations on CERTs, but instead adopt a law on information security and, thereby, in a broader context, define rights and obligations of all counterparts in the field. CERTs in EU Member States are usually established by govern-

ment decision. As previously recognised, the necessity of adopting a law on information security in Bosnia and Herzegovina is beyond question; BIH CERT's establishment contributes to the actualisation and acceleration of the adoption of the law. On the other hand, the efficiency of this model is questionable, since one cannot estimate the time required for regulation adoption. As well, the financial and human resources in the context of this model are difficult to plan or acquire in this period of crisis, since everything must be built from scratch. In that situation, the quality of BIH CERT information systems and communication would be strongly affected.

The second model may use the existing Law on Ministries and Other Administrative Bodies in Bosnia and Herzegovina for establishing BIH CERT.[58] Namely, according to competences defined by Articles 10 and 14 of the Law, BIH CERT may be incorporated within the Ministry of Transport and Communication, or within the Ministry of Security. In this case, the structure of BIH CERT may be regulated by the decision of the Council of Ministers, on which basis one may estimate the implementation time, i.e. establishment efficiency. In this case, BIH CERT would receive financial and administrative support from the existing resources of the corresponding ministry.

In addition to establishing BIH CERT, the Action Plan suggests forming a coordination body at the Council of Ministers with primary task to solve and mitigate existing problems through recommendations and support in the process of establishing BIH CERT and other CERTs in the country. It would publish mandatory recommendations to stakeholders, suggest adoption of regulations harmonised with EU and NATO standards and guidelines, insist on harmonisation of existing laws, coordinate cybersecurity activities between ministries and law enforcement agencies, suggest and initiate media campaigns and similar activities with the aim of raising awareness, and in general perform activities related to BIH CERT.[59]

However, the procedure of institutional establishment of BIH CERT has not yet started, because opposite political interests and stances in Bosnia and Herzegovina have affected the adoption of the previously described Action Plan and halted progress in this important apolitical field. On the other hand, it is only a question of time until the documents will be adopted and activities towards ensuring cybersecurity in Bosnia and Herzegovina reinitiated. That will be accomplished firstly due to EU recommendations and prerequisites the country will need to fulfil in order to accede to the EU, which is the main foreign policy objective of the country. Secondly, this project has no political dimension and the proposed structure of BIH CERT, together with its mission, activities and goals, is flexible and acceptable for all parties in Bosnia and Herzegovina. As stated, BIH CERT is envisioned as an expert body of an advisory and coordinating nature. Moreover, in the international context, the establishment of such a body in Bosnia and Herzegovina is desirable, because cyber threats know no geographical and political borders.[60]

Further on, besides the BIH CERT (to be established on the state level), the Department for Information Security within the Agency for Information Society of Republic of Srpska became operational in June 2015.[61] This Department was created by the Law on Information Security[62] with primary task to coordinate the prevention and protection from computer security incidents and expert supervision of implementation of measures and standards of information security in Republic of Srpska. This security unit closely cooperates with relevant departments in the Ministry of Interior of Republic of Srpska, especially the Unit for Preventing High-tech Crime.[63] The Unit is competent to investigate offenses committed against computer systems, crimes involving technology and to perform digital forensics. On the other hand, computer security incidents in the other Bosnia and Herzegovina entity are handled by the Crime Police Department of the Federal Police Administration since there is no specialised unit exclusively established to deal with high tech crime in the Federation of Bosnia and Herzegovina. This Department has relevant but insufficient capacity, and has at its disposal the services of the Forensics and Support Centre within the Federal Police Administration. Finally, Brčko District currently does not have cybersecurity capacity and no high tech crime unit has been established due to its specific territorial and subject matter jurisdiction.

Aside from the subject of cybersecurity units in governmental institutions, Bosnia and Herzegovina hosts the Southeast Europe Cybersecurity Center (SEECSC)[64] – a research and development unit at the American University in Bosnia and Herzegovina, which offers quality cybersecurity education, training, research, services and infrastructure to overcome not only challenges of security and protecting the cyberspace in Bosnia and Herzegovina, but in the region as well. The training and education is realised through professional trainings, and master and doctoral programmes in cybersecurity. The research activities of the centre include cryptography, cybersecurity policy, digital forensics, hardware security, information assurance, information security, mobile device security, software security, systems security, threat analysis, and network and wireless security. In addition, the services that the centre offers are realised with security, intelligence and defence institutions in Bosnia and Herzegovina and include digital forensics, incident response, cyber intelligence, information assurance security, security assessment, etc. Further on, the banking sector in Bosnia and Herzegovina is in the process of forming a security unit on the state level for the purpose of exchanging experiences, information and best practices between IT administrators and experts that work in banks' information security departments.

Internal and International Cybersecurity Cooperation in Bosnia and Herzegovina

Internal cooperation on cybersecurity issues in Bosnia and Herzegovina, which includes cooperation between public, private, academic, industry and government sector, is not satisfactory. In general, the nature of this cooperation is informal. For example, different degrees of cooperation exist between law enforcement agencies on different state levels and currently existing 76 ISPs for the purpose of investigation. However, this cooperation needs to be raised on a higher level and formalised. The lack of adequate legal regulations has been identified as the main cause of poor cooperation, together with the lack of will and initiative to train police personnel and employees of ISPs, and lack of specialised equipment.

In addition, as already described, SEECSC realises the cooperation among all stakeholders through cooperation with government security, intelligence and defence institutions, universities, and the banking sector. However, when it comes to cooperation between public and academic sector, in general it may be characterised as dissatisfying. There are many possibilities to gain grants through projects for strengthening cybersecurity capabilities in Bosnia and Herzegovina with no expected investments from the country's budget. However, the need for a central contact point on the state level has been recognised as a single prerequisite when applying for these funds. Namely, due to the lack of a central point and the extremely weak cooperation between institutions and universities, or lack of it, the funds remain unused.[65]

Further on, when it comes to international cooperation in the field of cybersecurity, there is cooperation with foreign specialised units through Interpol and international legal assistance routes. The procedure for providing mutual legal assistance in criminal matters follows the provisions of the European Convention on Mutual Legal Assistance in Criminal Matters and its Protocols to which Bosnia and Herzegovina is a Party, as well as the provisions of multilateral and bilateral agreements on legal assistance that are binding for Bosnia and Herzegovina. The procedure for providing mutual legal assistance in criminal matters is carried out in accordance with the provisions on the Law on Mutual Legal Assistance in Criminal Matters, in force since 15 July 2009. The Ministry of Justice of Bosnia and Herzegovina is the central liaison authority in the procedures for providing mutual legal assistance in criminal matters. In 2010, the Ministry of Justice acted upon requests in two cybercrime related cases. An expedited procedure is possible regarding foreign requests, if the foreign authority requests such a procedure. In such urgent cases requests may be delivered through Interpol or Eurojust; provided that a copy of the request is submitted to the Ministry of Justice of Bosnia and Herzegovina. Police authorities in Bosnia and Herzegovina directly cooperate with police authorities of other countries, exchange information

and are able to participate in establishing joint investigative teams with other countries on the basis of the Law on Mutual Legal Assistance in Criminal Matters.[66]

In addition, contacts with relevant international cybersecurity organisations have been established, but it is impossible for Bosnia and Herzegovina to become a member until the legislation is harmonised and corresponding bodies (not necessarily operational) are established.

Cybersecurity Technical, Law Enforcement and Judicial Qualification Level in Bosnia and Herzegovina

The technical qualification level of organisations and institutions in Bosnia and Herzegovina in terms of cybersecurity may be rated as acceptable. That is the area where the organisations and institutions in Bosnia and Herzegovina stand the best in comparison to legal regulations or level of staff training. Of course, this area would also need improvement, but in the context of cybersecurity capability development, significant investments as well as a start from scratch are not required.

When it comes to the qualification level of the corresponding staff in police and judicial and prosecutorial institutions, it can be characterised as insufficient. The Agency for Training and Advanced Professional Training of Personnel[67] is the competent body for developing and delivering basic and specialised training courses to law enforcement agencies within the Ministry of Security of Bosnia and Herzegovina. There is no documented training strategy at the state level covering the areas of cybercrime investigation and digital forensics. New recruits are not taught how to recognise and deal with electronic devices that may contain evidence. Cybercrime specialists do not have individual training plans and there are no arrangements in place with academic or industry bodies to support development and delivery of cybercrime training, but those are informal and based on personal efforts and interests. Namely, several police employees working on cybersecurity issues have been trained by international specialists, but that is hardly enough. In general, training on cybersecurity topics should be increased and structurally distributed to the lowest level of police personnel. Possibly, the recently signed Agreement between the Ministry of Security of Bosnia and Herzegovina and CEPOL on training police officers in accordance with European standards will make a difference.

However, at the state level it is considered beneficial to have specialised training courses on:[68]

- Dealing with electronic devices and recognition of devices which may contain evidence of crime;
- Search of computers and other electronic equipment (mobile phones, etc.);

- Analysis of digital evidence and its presentation;
- Use of the Internet as an open source tool in investigation;
- Interception of electronic messages;
- Training on various types of cybercrime including paedophilia;
- IT system protection and security.

It is also recognised that training of trainers is important to ensure that knowledge may be passed to participants in basic and specialised subjects on the listed topics. It is also considered beneficial for specialists in this type of crimes to receive training with others from jurisdictions with similar legal systems, in the form of workshops, joint training sessions, etc. in order to educate each other and exchange experience with a view of improving future work on individual cases. It is further considered beneficial for similar activities to be held involving different players in the criminal justice system within the country.

On the entity levels, within the entities' ministries of interior there are the police academies which develop and deliver appropriate types of education of police officers. Training courses in computer crime are rare and often organised with the support of foreign governments and international organisations. There is no documented cybercrime training strategy and no information is provided with regard to subject area qualifications available to staff. Also, there are no official arrangements with academia or industry to support this type of training.

Further, in terms of judicial and prosecutorial institutions, training is not conducted at the state level, but on the entity levels there is the Centre for Education of Judges and Prosecutors and Judicial Commission of Brčko District, which does not deliver cybercrime education. However, there are plans for cybersecurity training of the corresponding staff. The staff also expressed interest in joint trainings at the international level. The same recognition exists with regard to joint training activities including the various players in the criminal justice system. Also, it has been noticed that employees that had been educated in the field of cybersecurity have changed their positions. Thereby, invested efforts and resources are wasted and in the future the government should select the trainees more carefully.

Conclusion

Internet and ICT have become the most important components in everyday life, altering behaviour patterns and in many aspects making our lives simpler. Upcoming IoT will have additional positive influence on our QoL. However, even now, society is extremely vulnerable to disturbances that may affect the functioning of the Internet and ICT systems, and thereby jeopardise the reliability and security of the infor-

mation they contain. The situation tends to become even more complicated when IoT takes effect and cyber threats exceed the perimeter of information security and include physical security, existence and health. The world has shyly started to raise questions and perceive problems regarding the IoT, QoL and security issues in the cyber space in order to find the appropriate solutions on time. Bosnia and Herzegovina needs to take place in these processes and newly opened research fields.

This paper provided an overview of the current situation in Bosnia and Herzegovina regarding security in cyber space. Cybersecurity is not among the priorities in Bosnia and Herzegovina. Namely, decentralised and complex traditional security management structure with a number of different organisations leads to unsynchronised and bad decisions, which further leads to greater complexity and results in Bosnia and Herzegovina being more susceptible to risks and threats in the cyber domain. The scarcity and disharmony of legal regulations in field of cybersecurity, together with lack of cybersecurity units, their cooperation, and staff qualification additionally aggravates this situation, while opposite political stances, interests and goals in Bosnia and Herzegovina, together with the mentality reflected in "the boss" question tend to block, halt, aggravate and discourage the little optimism, goodwill and initiative that exist. In other words, Bosnia and Herzegovina has the capacities, but lacks the will, determination and devotion to regulate cyber issues. Instead of embracing worldwide and generally accepted cybersecurity solutions (e.g., in terms of cybersecurity related legislation, units, etc.) and catching the pace, the country offers difficulties and issues embodied in above discussed problems and needs to work on its readiness to contribute to the safety of IoT and cyber space, and consequently improve citizens' QoL.

However, it is only a question of time until the activities towards ensuring cybersecurity in Bosnia and Herzegovina will be enhanced. That will be accomplished firstly due to EU recommendations and prerequisites the country will need to fulfil in order to accede to the EU – the main foreign policy objective of the country. Thereby, the government's commitment to EU and NATO integration would be confirmed and no longer characterised as declarative. Secondly, the opportunity for reinitiating the activities lies in the fact that cyber threats and attacks, which know no geographical and political borders, will eventually happen to someone important in the country. Those activities are aimed at catching the pace with world trends in cybersecurity: harmonization of legislation (e.g., Law on Information Security), adoption of national cybersecurity strategy, establishment of more cybersecurity units together with a national umbrella CERT body (BIH CERT), which would mutually cooperate and connect with relevant international bodies in order to exchange information, knowledge and best practices, identification and protection of critical information infrastructure, increasing the qualification level of cybersecurity related staff, etc. Finally, the en-

hancement of cybersecurity will send a positive signal to citizens and the international community and bring other benefits, e.g., economy boost.

Notes:

[1] Sabina Baraković, "Multidimensional Modelling of Quality of Experience for Mobile Web Browsing," PhD dissertation (Zagreb: University in Zagreb, 2014).

[2] "The Internet of Things," Gartner IT, accessed on 20 May 2015, available at http://www.gartner.com/it-glossary/internet-of-things.

[3] Kevin Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 22 June 2009, available at http://www.rfidjournal.com/articles/view?4986.

[4] EY, "Cybersecurity and the Internet of Things," March 2015, available at http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf.

[5] Sabina Baraković, Mladen Mrkaja, Amir Husić, Adnan Kulovac, and Jasmina Baraković Husić, "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime by Establishment of BIH CERT Body," in *Cyber Security and Resiliency Policy Framework*, ed. Ashok Vaseashta, Philip Susmann, and Eric Braman (IOS Press, 2014), 65-81, http://dx.doi.org/10.3233/978-1-61499-446-6-65.

[6] Ollie Whitehouse, "Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond," NCC Group, 20 April 2014, available at https://www.nccgroup.trust/uk/our-research/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/.

[7] Sabina Baraković, "Multidimensional Modelling of Quality of Experience for Mobile Web Browsing," PhD dissertation (Zagreb: University in Zagreb, 2014).

[8] "Cybercrime situation report," CyberCrime@IPA – EU/COE Joint Project on Regional Cooperation against Cybercrime, March 2011; Sanja Šabanadžović, "Cyber criminal u Bosni i Hercegovini: Od iznuda i krađa bankovnih kartica do dječije pornografije," *Radio Sarajevo*, 21 April 2015, available at http://radiosarajevo.ba/novost/186443/cyber-kriminal-u-bosni-i-hercegovini-od-iznuda-i-krada-bankovnih-kartica-do-djecije-pornografije.

[9] Official Website of the Ministry of Security of Bosnia and Herzegovina, http://www.msb.gov.ba.

[10] Constitution of Bosnia and Herzegovina.

[11] The Law on Ministries and Other Administrative Bodies in Bosnia and Herzegovina," Official Gazette of Bosnia and Herzegovina, 2/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09.

[12] Official Website of the Directorate for Coordination of Police Bodies, http://www.dkpt.gov.ba.

[13] Official Website of the Border Police of Bosnia and Herzegovina, http://www.granpol.gov.ba.

[14] Official Website of the State Investigation and Protection Agency, http://www.sipa.gov.ba.

[15] Official Website of the Agency for Forensics and Expert Examination, http://afiv.gov.ba/.

[16] Official Website of the Personnel Education and Professional Development Agency, http://www.aeptm.gov.ba.

[17] Official Website of the Police Support Agency, http://www.psa.gov.ba.

[18] Official Website of the Service for Foreigners' Affairs, http://www.sps.gov.ba.

[19] Official Website of the Federal Police Administration, http://www.fup.gov.ba.

[20] Official Website of the Ministry of Interior of Republic of Srpska, http://www.mup.vladars.net.

[21] Official Website of the Police of Brčko District, http://policijabdbih.gov.ba.

[22] Baraković et al., "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime."

[23] Convention on Cybercrime, CETS No. 185, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

[24] Stabilisation and Association Agreement between Bosnia and Herzegovina and the European Commission, 2008, http://www.dei.gov.ba/bih_i_eu/ssp/default.aspx?id=1172&langTag=en-US.

[25] Decision on Ratification of the Cybercrime Convention, March 2006, http://www.fup.gov.ba/wp-content/uploads/2012/01/Konvencija-o-cyber-kriminalu-Budimpesta.pdf.

[26] Baraković et al., "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime."

[27] Strategy for Establishment of CERT (Computer Emergency Response Team) in Bosnia and Herzegovina, Council of Ministers of Bosnia and Herzegovina, July 2011, available at http://www.msb.gov.ba/dokumenti/strateski/default.aspx?id=6248&langTag=bs-BA.

[28] Strategy for Combating Organized Crime 2014-2016, available at http://msb.gov.ba/PDF/Strategija_za_borbu_protiv_organiziranog_kriminala_u_BiH_2014_2016.pdf.

[29] Memoranda of Cooperation and Mutual Assistance between the Ministry of Security of Bosnia and Herzegovina and the Association for Protection of Audiovisual Works in Bosnia and Herzegovina, http://msb.gov.ba/vijesti/saopstenja/default.aspx?id=9600&langTag=bs-BA.

[30] Action Plan for Protection of Children and Prevention of Violence over Children via Information Communication Technologies in Bosnia and Herzegovina 2014-2015, http://msb.gov.ba/PDF/140605_Nasilje_bosnanski_SG_ver2.pdf.

[31] "CEPOL Signs Working Agreement with Bosnia and Herzegovina," 3 December 2014, available at https://www.cepol.europa.eu/media/news/20141203/cepol-signs-working-arrangement-bosnia-and-herzegovina.

[32] Decision on Legal Interception, November 2006, www.mkt.gov.ba/dokumenti/komunikacije/zakoni/podzakoni/default.aspx?id=3657&langTag=bs-BA.

[33] Criminal Law, Official Gazette of Federation of Bosnia and Herzegovina, 36/03, 37/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14; Criminal Law, in Official Gazette of Republic of Srpska, 49/03, 108/04, 37/06, 70/06, 73/10, 1/12, 67/13; Criminal Law, in Official Gazette of Brčko District, 10/03, 45/04, 06/05, 21/10, 52/11.

[34] Criminal Law in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 3/03.

[35] Criminal Procedural Law, Official Gazette of Federation of Bosnia and Herzegovina, 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13, 59/14; Criminal Procedural Law, Official Gazette of Republic of Srpska, 53/12; Criminal Procedural Law," in Official Gazette of Brčko District, 10/03, 48/04, 06/05, 12/07, 14/07, 21/07, 27/14.

[36] Law on Electronic Signature, Official Gazette of Republic of Srpska, 59/08; Law on Electronic Document, Official Gazette of Republic of Srpska, 110/08; Law on Electronic Management," in Official Gazette of Republic of Srpska, 59/09.

[37] Law on Information Security, Official Gazette of Republic of Srpska, 70/11.

[38] Criminal Law in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 3/03.

[39] Criminal Procedural Law, Official Gazette of Bosnia and Herzegovina, 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13.

[40] Law on Protection of Personal Information, Official Gazette of Bosnia and Herzegovina, 32/01, 49/06.

[41] Law on Protection of Classified Information, Official Gazette of Bosnia and Herzegovina, 54/05.

[42] Law on Communications, Official Gazette of Bosnia and Herzegovina, 31/03.

[43] Law on Electronic Signature, Official Gazette of Bosnia and Herzegovina, 91/06.

[44] Law on Electronic Legal and Business Transactions, Official Gazette of Bosnia and Herzegovina, 126/07.

[45] Law on Prevention of Money Laundering and Financing of Terrorism, Official Gazette of Bosnia and Herzegovina, 47/14.

[46] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, February 2013, available at http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[47] Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union, February 2013, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF.

[48] Baraković et al., "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime."

[49] Miralem Porobić and Mirsad Bajraktarević, "Cybercrime, pranje novca i finansijske istrage," February 2012.

[50] Criminal Law in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 3/03.

[51] Strategy for Establishment of CERT (Computer Emergency Response Team) in Bosnia and Herzegovina.

[52] Decision on Establishment and Appointment of Expert Working Group for Conduction of All Necessary Preparations for the Formation of CERT Body in Bosnia and Herzegovina, December 2011, available at www.sluzbenilist.ba/Sluzbeni%20dio/Sluzbeni%20glasnik%20Bih/2012/broj6/Broj006.pdf.

[53] Akcioni plan uspostave BIH CERT-a," December, 2011.

[54] Sabina Baraković, "Establishment of CERT Body in Bosnia and Herzegovina," DCAF Young Faces 2014 – Cybersecurity Winter School for the Western Balkans, December 2014, available at www.dcaf.ch/content/download/234384/3678160/version/1/file/YF14PolicyBrief-BARAKOVIC.pdf.

[55] Strategy for Establishment of CERT (Computer Emergency Response Team) in Bosnia and Herzegovina; Akcioni plan uspostave BIH CERT-a, December 2011; Sabina Baraković, "Establishment of CERT Body in Bosnia and Herzegovina."

[56] Akcioni plan uspostave BIH CERT-a, December 2011; Sabina Baraković, "Establishment of CERT Body in Bosnia and Herzegovina."

[57] Baraković, "Establishment of CERT Body in Bosnia and Herzegovina."

[58] Law on Ministries and Other Administrative Bodies in Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, 2/03, 26/04, 42/04, 45/06, 88/07, 35/09, 59/09, 103/09.

[59] Baraković, "Establishment of CERT Body in Bosnia and Herzegovina."

[60] Baraković, "Establishment of CERT Body in Bosnia and Herzegovina."

[61] Odjeljenje za informacionu bezbjednost, http://oib.aidrs.org/.

[62] Law on Information Security, Official Gazette of Republic of Srpska, 70/11.

[63] Agency for Information Society of Republic of Srpska, "Počelo sa radom Odjeljenje za informacionu bezbjednost (OIB)," accessed on June 29, 2015, www.aidrs.org/pocelo-sa-radom-odjeljenje-za-informacionu-bezbjednost-oib/.

[64] Southeast Europe Cybersecurity Center, https://www.seecsc.org.

[65] Baraković et al., "Overview of the Current Situation in Bosnia and Herzegovina with Focus on Cyber Security and Fighting Cyber-Crime."

[66] "Cybercrime situation report," CyberCrime@IPA – EU/COE Joint Project on Regional Cooperation against Cybercrime, March 2011.

[67] Official Website of the Personnel Education and Professional Development Agency, http://www.aeptm.gov.ba.

[68] "Cybercrime situation report," CyberCrime@IPA - EU/COE Joint Project on Regional Cooperation against Cybercrime, March 2011.

Sabina Baraković is employed as a senior adviser at the Ministry of Security of Bosnia and Herzegovina, in the Sector for Informatics and Telecommunication Systems. She received her Dipl. Ing. and Ph.D. degrees in electrical engineering from the University of Tuzla, Faculty of Electrical Engineering in 2009 and the University of Zagreb, Faculty of Electrical Engineering and Computing in 2014. She also works as Assistant Professor at the university in Sarajevo. Her research interests include cybersecurity, Quality of Life (QoL), Quality of Experience (QoE), multimedia and mobile web-based applications, Next Generation Networks (NGN) and Quality of Service (QoS). She is currently involved in a number of projects, including Building cyber resilient societies in the region of SEE, EU COST Action IC1003 (European Network on Quality of Experience in Multimedia Systems and Services, QUALINET), EU COST Action IC1304 ACROSS (Autonomous Control for a Reliable Internet of Services), EU COST Action IC1303 (Algorithms, Architectures, and Platforms for Enhanced Living Environments – AAPELE), etc. She has published over 20 scientific and professional papers.

Jasmina Baraković Husić is employed by BH Telecom, Joint Stock Company, Sarajevo since 2005. She has been working as professional associate in the Directorate BH Mobile. She has graduated from the University of Tuzla, Faculty of Electrical Engineering in 2004. She spent six months at the Munich University of Technology as a scientific researcher during the same year. She has defended doctoral thesis in the field of signaling information transmission at the University of Zagreb, Faculty of Electrical Engineering and Computing in 2009. She joined the University of Sarajevo, Faculty of Electrical Engineering in 2011, where she works as Assistant Professor at the Department for Telecommunications. She also teaches at the Department of Communications of the Faculty of Traffic and Communication. Her research concerns a variety of topics in quality of service (QoS), quality of experience (QoE), multimedia networking and signaling, and cybersecurity. She has published 2 books and more than 30 science and professional papers based on her research interests. She is member of IEEE Communication Society and Bosnian-Herzegovinian Society for Telecommunications – BHTEL.