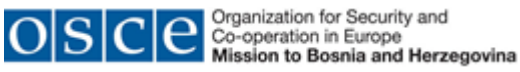
GUIDELINES FOR A STRATEGIC CYBERSECURITY FRAMEWORK IN BOSNIA AND HERZEGOVINA

Sarajevo, October 2019

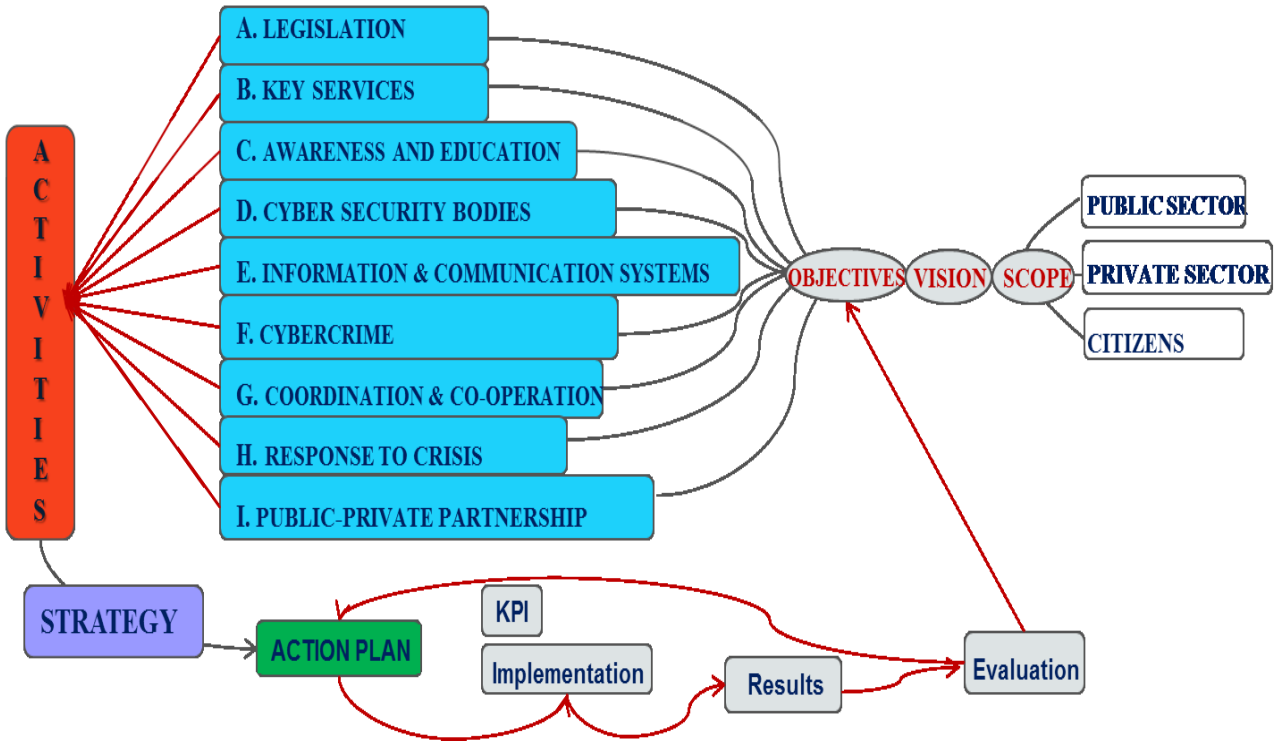


The development of this document was supported by the OSCE Mission to BiH. Any view, statement, or opinion expressed in this document, which is not specifically attributed to the OSCE Mission to BiH, does not necessarily reflect the official policy of the OSCE Mission to BiH.

Contents

VISION (5 years)

In line with the realistic needs, potential threats, as well as international commitments and standards in the area of cyber security, the Vision of the Strategic Cybersecurity Framework in Bosnia and Herzegovina shall ensure a strategic and legal framework and competencies, as well as it shall improve procedures and techniques to protect information and communications systems and end users in cyber space. The Vision shall achieve risk reduction, while respecting privacy, and shall promote the technical innovation, facilitates communication, economic development and transparency, as well as the security of the overall society.



No.1

I. Understanding the Strategic Framework Guidelines

Contemporary society relies heavily on the benefits and innovations offered by information and communication technologies, which have become indispensable factors in all spheres of life and activity. The development of communications technologies is happening at a rapid pace globally by connecting people and devices across the globe to a comprehensive system we call the Internet. Civil services, critical infrastructure, including the financial sector, the energy sector, the military and security sectors, then hospitals, services, companies, schools and citizens, are increasingly and irreversibly dependent on interconnectedness and the global network. Global connectivity, the development of technology and the digital environment also mean that the effects of these developments are comprehensive - from positive and affirmative to those at risk and negative. Endangerment of the cyber[1] space security, be it cyber threats, terrorism, escalation of relations between states, illegal trade, all types of cybercrime and abuse, has long been not within the scope of local or national, but rather international. Cyber space is now increasingly recognized as a new area of conflict, and countries include cyber elements of military doctrine or the development of offensive cyber capabilities and cyber military commands in their traditional elements. International legislation is also accelerating globally to guarantee a safe, open and stable cyber space.

Bosnia and Herzegovina, as a member of international organizations, has committed itself to uphold the obligations, principles and standards arising from membership in these organizations, be it the United Nations (UN), the Organization for Security and Co-operation in Europe (OSCE), regional initiatives or commitments on the path to accession to the European Union. One of Bosnia and Herzegovina's international commitments is to implement the OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies adopted by the OSCE Permanent Council, to ensure open, interoperable, secure and reliable Internet in OSCE countries, and to reduce the risk of misperception and possible outbreak of political and military tension or conflict. Bosnia and Herzegovina's strategic goal is to join the EU through accession negotiations to full membership. One of the requirements during this process is an adequate level of cyber security. Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security for network and information systems across the Union, also known as NIS Directive[2] (*EU Network and Information Security Directive*), inter alia requires that each Member State adopts its own Information and Communication Systems Security

[1] The term "cyber" is used throughout this document to mean a space that is widespread and interconnected with digital technologies, established with the assistance and mediation of computer-digital technology. The term cyber space is used today for everything on the Internet.

[2] NIS Directive: (Eng.) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Avvailable at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Strategy. By ratification of the Council of Europe Convention on Cybercrime (Budapest Convention), there is a need to combat cybercrime in the context of these international commitments[3]. Bosnia and Herzegovina is a signatory to the Stability Pact - an initiative for e-South East Europe - eSEE 2007, which promotes regional co-operation and the growth and development of electronic communications. Failure to comply with these obligations and none participation in efforts to implement common security measures can have adverse consequences for Bosnia and Herzegovina, not only in the critical technical domain, but also in diplomatic and political terms.

The number of devices connected to the Internet is growing exponentially, as is the number of active Internet users[4], which indicates a positive development of the BiH society. Cyber space offers many opportunities for growing economies and citizens, and helps closing the gap between rich and poor. Current, as well as development facilities need to be protected, given the exposure and growing threats in cyberspace.

However, as stated in the European Commission Progress Report on Bosnia and Herzegovina as early as 2016, "Bosnia and Herzegovina does not have a comprehensive strategic approach to address cybercrime and cyber security threats." It states that the response to cyber security threats, existing cybercrime capabilities, as well as the capacity of teams to prevent and protect against cyber incidents and threats to the security of public information systems (CERT / CSIRT) need to be strengthened[5].

The existing human and resources capacities and capacities of the organizations are not sufficient to provide the required level of security in cyber space in Bosnia and Herzegovina. Different levels of government have different levels of preparedness, which have led to different approaches to cyber security issues within Bosnia and Herzegovina. The result is an unequal level of user protection, both in the public and private sectors, which undermines the overall level of protection of cyber space, vulnerability to threats and attacks, and the inability to act, co-operate and coordinate with other countries in the region and the world in a timely manner. Bosnia and Herzegovina is the only country in Europe that does not have a CSIRT system in place (a system to assist Internet users in Bosnia and

[3] Documents: Convention on Cybercrime, Budapest, 23 November 2001, came into force on 01 July 2004, came into force in relation to BiH on 01 September 2006; published in the "Official Gazette of BiH"– International Treaty No: 06/2006); Additional Protocol on the Convention on Cybercrime, Concerning the Criminalisation of Acts a Racist and Xenofobic Nature Commited through Computers Systems, Strazbourg, 28 January 2003, came into force on 01 March 2006, came into force in relation to BiH 01 September 2006; published in the "Official Gazette of BiH" – International Treaty No. 06/2006);

[4] Report on the Results of the RAC Annual Survey of Users licenses for Providing Internet Services in Bosnia and Herzegovina for 2018 - estimates that in 2018 there were 3,195,294 Internet users, i.e. the Internet usage rate in Bosnia and Herzegovina for 2018 is 90,49%. Availabe at: https://docs.rak.ba//documents/ea9d822c-b1dc-4ad9-b2d9-735dc6c8ea91.pdf

[5] CERT (Eng. Computer Emergency Response Team) or CSIRT (Eng. Computer Security Incident Response Team)

Herzegovina in implementing pro-active measures to reduce the risk of computer-security incidents and to help counteract the consequences of computer-security incidents).[6]

In light of its commitment to the future EU membership, Bosnia and Herzegovina will need to adopt new legislation and align existing cyber security legislation. The governing documents are the EU General Data Protection Regulation[7] and Directive of the European Parliament and of the European Council on Measures for a High Common Level of Security for Network and Information Systems across the European Union ("NIS Directive"). Although EU regulations indicate a horizon for future efforts, OSCE confidence-building measures in cyber space[8], are already politically binding on Bosnia and Herzegovina.

Global threat protection should be comprehensive and harmonized. In order to ensure coherence, there is a need for a strategic framework. The cyber security strategic framework provides guidelines for action to all actors, and it includes the administrative and technical aspects of cyber security, defines the vision and goals that are achieved through its implementation. It is possible to create coordinated action plans based on the guidelines for the strategic framework and future implemented strategies, and the implementation of it will reach the set objectives, i.e. reduce cyber security risk.

This Strategic Framework has applied the positive experiences and best practices of countries that have already adopted and implemented National Cyber Security Strategies. The document defines a minimum number of objectives and activities that will lead to an effective and enforceable strategic framework, i.e. to tangible and measurable results of cyber security management. Such management will be reflected in the implementation of the project life cycle phases, which relate to: development, implementation, evaluation and adaptation of the Strategic Framework. Thus, this document represents a strategic framework for establishing the effective cyber security system. The Strategic Framework is based on the NIS directive, the ENISA Best Practices Guide, as well as on the positive practices of EU countries and countries in the region that have adopted National Strategies and have established appropriate cyber-attacks response mechanisms.

This document was produced within the framework of an Informal Working Group of Experts from different administrative levels and areas of action in Bosnia and Herzegovina, gathered under the auspices of the OSCE Mission to Bosnia and Herzegovina. The original aim of addressing the threats

[6] ENISA, CSIRTs by Country - Interactive Map, available at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

[7] DIRECTIVE (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on o the protection of individuals with regard to the processing of personal data and the free movement of such data, and the repeal of the Directive 95/46/EU (General Data Protection Regulation); Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679

[8] OSCE DECISION No. 1202 OSCE Confidence-Building Measures to Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies; PC.DEC/1202, of 10 March 2016; Available at: https://www.osce.org/pc/227281?download=true

and protection in the digital world and the initiation of a comprehensive discussion of the strategic framework and security guidelines, resulted- through the expressed need of all stakeholders- in a concrete proposal, or the document that presents strategic guidelines for the harmonization of existing and development of future cyber security strategies in BiH, which is in line with the Recommendations and Conclusions of the OSCE 11th Review Conference on Implementation of the OSCE and UN Commitments of Bosnia and Herzegovina.

The document is subject to ongoing analysis, evaluation and upgrade in line with the cycles of development and implementation of strategic goals in the cyber domain.

II. Scope and Objectives

SCOPE

The sectors of society covered by the Strategic Cyber Security Framework in Bosnia and Herzegovina are as follows:

1. Government institutions, the public sector and bodies representing cyber-space users in various ways and those obliged to implement measures arising from the Strategic Framework.

2. Private sector – legal entities that are subject to special regulations on critical information and communication infrastructures, as well as all other legal entities, i.e. business entities that in various ways represent users of cyberspace and are obliged to implement measures arising from the Strategic Framework.

3. Citizens who represent users of communications and information technologies and services, and who in different ways reflect the security situation in cyberspace. The Strategic Framework also applies to those citizens who do not actively use cyber space, but their personal information is contained therein.

OBJECTIVES

Overall Objective

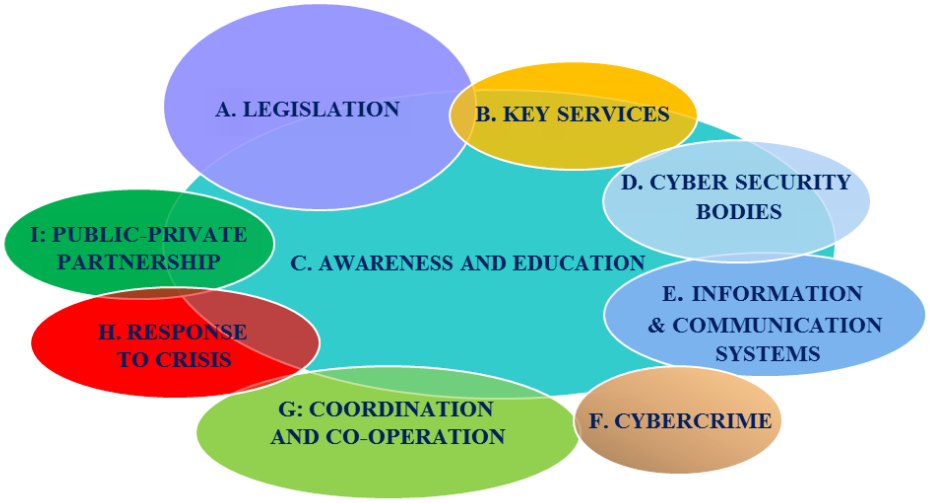
The overall objective defined in this document is to enhance the security of cyber space in function of the progress of the society as a whole. This objective- safer cyber space- shall be achieved through capacity building and the development of mechanisms for prevention, detection and response to security challenges.

Strategic Objectives:

A. **A systematic approach to the harmonization and development of cyber security legislation is ensured;**
B. **Secured Information and Communication Systems of the Key Services Providers;**
C. **Raising the Awareness and Knowledge of Cyber Security;**
D. **Functional Bodies in charge of Securing, Strengthening and Improving Cyber Security;**
E. **Improved Security and Resilience of Information and Communication Systems;**
F. **Enhanced Capacity to Combat Cybercrime;**
G. **Effective Cyber Security Co-operation established in International, Regional and National Frameworks;**
H. **Capacity Built to Adequately Respond to Crisis;**
I. **Public- Private Partnership Established.**

The Strategic Objectives shall be implemented through appropriate legislative, regulatory and operational measures with the aim of achieving and maintaining the high level of security of information and communication systems. Each of these strategic objectives is explicated by sub-objective and elaborated to the level of activities required for its achievement.

Cyber Security Strategies- to be adopted at all levels of government in accordance with constitutionally and legally defined competencies- should at a minimum contain the stated strategic objectives.



No. 2

OBJECTIVE A: A systematic approach to the harmonization and development of cyber security legislation is ensured

Legislation is the fundament for building on the protection measures and the definition all obligations for all participants in the cyber security system. Circumstances are changing rapidly in cyber security, so it is important to ensure that legislation also adapts to these changes swiftly enough. Changes should be harmonized and implemented at all administrative levels, from laws to by-laws.

A1: A review of existing legislation, policies, regulations and opportunities completed

The first step, before any change, is to review what the existing legal solutions offer in cyber security. In addition to the laws directly related to cyber security, there may be some related to the general security, electronic communications, key services and critical infrastructure that regulate cyber security issues for some sectors. Apart from laws, there may be cyber security policies and strategies. Sectors that have regulatory bodies may have their own regulations that may also define some cyber security issues. All such existing elements should be used to implement measures to improve cyber security immediately, without waiting for new, yet uncreated laws or amendments to the existing ones. Only after establishing a complete picture of cyber security legislation should harmonization and changes be made, where necessary, prioritized and in line with competencies.

The activities pursued by the foregoing are as follows:

1. Review existing cyber security policies in BiH;
2. Review existing cyber security regulations in BiH;
3. Analyse what existing policies and regulations already allow for cyber security.

A2: Harmonized legislation with international cyber security regulations, obligations and standards

There are a number of international regulations in the area of legislation for cyber security, as well as standards that can be helpful and with which it is good to have legislation harmonized with, even if there is no current formal obligation. The cyber security standards developed by international bodies such as ISO, ITU, ENISA, NIST and others are the result of lengthy processes and lessons learned. This knowledge and experience should be used for the common good and security. The existing cyber security legislation identified during the review process should be analysed from the aspect of compliance with international regulations and standards, especially taking into account obligations assumed through signed international treaties and future obligations that will be current within Bosnia and Herzegovina's pre-accession negotiations with the European Union. Mismatches should be identified and where possible remedied. This should be the first step in amending existing legislation. Some of the standards cover only specific areas and should therefore be applied and referenced when analysing legislation in the field. It is necessary to monitor the development of a defined set of legislation and standards, to align domestic legislation and standards with the changes that have occurred.

The activities pursued by the foregoing are as follows:

1. Define a set of international bodies or their organizational units with whose regulations, obligations or standards is needed to be aligned with;
2. Define a set of cyber security regulations, obligations or standards to be harmonized individually and by sector;
3. Analyse domestic legislation’s compliance with international regulations, obligations or standards;
4. Develop necessary legal solutions in line with international commitments and standards and eliminate inconsistencies in existing ones, but all in line with competencies;
5. Keep abreast of and comply with changes to international commitments and standards.

A3: Security balanced with privacy and data protection

The implementation of cyber security measures must not jeopardize the privacy of citizens, which is a fundamental human right and freedom. All citizens have the right to privacy and protection of personal data. This should be taken into account when enacting new and amending existing laws, as well as when planning and implementing the measures of protection.

The activities pursued by the foregoing are as follows:

1. Ensure privacy and protection of personal data in accordance with the international standards, as well as with the EU General Data Protection Regulation (GDPR) in all steps of the strategy implementation.

OBJECTIVE B: Secured Information and Communication Systems of the Key Services Providers

Information and communication systems that enable the provision of services critical to the maintenance of critical social and economic activities should be specifically protected. The set of critical services and databases of critical importance, the list of providers of key services and databases and the critical information and communication infrastructure should be legally defined. Besides the definition, it is also necessary to prescribe the obligation to protect critical information and communication infrastructure for the providers of key services and databases. Minimum security measures should be prescribed for all key service providers and databases. These measures should be in line with the cyber security standards for the sector to which that operator belongs to. Each of the providers of key services and databases should take measures to reduce the risk to critical information and communication infrastructure. These measures should be the result of the analysis carried out in accordance with the prescribed risk analysis methodology. Key service and databases providers should be required to carry out a regular risk analysis. Also, key service providers should have their CSIRTs cooperating with other CSIRTs and bodies defined under Objective D in accordance with the NIS Directive.

B1: Legally defined key services and databases, their providers and critical information and communication infrastructure and the obligation to protect it.

Key services and databases should be defined by the legal framework. For each of the key services and databases, it is required to identify by law the providers that provide it and the participants responsible for the security of the key services and databases. The protection of the information and communication infrastructure of these providers- whose functioning of the key services and databases depends on- should be legally required.

Activities:

1. Adopt legislation on key services and databases, key service providers and critical information and communication infrastructure;
2. Prescribing the obligation to protect critical information and communication infrastructure to key service providers.

B2: Minimum security measures identified

Providers of key services belonging to the same sector or providing the same key service should have a coordinated approach to cyber security. This approach should be based on general international cyber security standards, and in particular those used in the sector. This allows for mutual understanding, verification of the enforcement by the competent authorities and exchange of information on best security practices and security incidents. Defining the minimum security measures required allows for the rational and targeted use of limited resources. These measures can be defined in a law that treats key services and their providers.

Activities:

1. Analysis of minimum required security measures by sector - key services;
2. Alignment with international security standards for the sector;
3. Update legislation as needed.

B3: Reduced risk and consequences for critical infrastructure from attacks or accidents

Reducing the risk reduces the potential for security threats and their consequences. In order to reduce the risk, it is necessary to carry out its analysis. Risk analysis is a comprehensive and complex process. In order to assist key services and databases providers and to ensure a coherent approach, it is necessary to adopt a methodology that should be used to analyse the risks across key services and sectors in line with competencies. Every provider needs to know what procedure to apply in order for his risk analysis to be complete. Each provider identifies its own information and communication systems whose compromising could jeopardize the provision of key services for which the provider is responsible. These systems should be subject to a risk analysis. Providers take risk mitigation measures based on this analysis. The entire risk analysis process should be documented and performed regularly at minimum prescribed intervals.

Activities:

1. Adopt risk analysis methodologies for all key service providers and databases by key services and sectors in line with competencies;
2. Each provider should identify the information and communication infrastructure critical to the provision of key services for which it is responsible;
3. Assess the risk of compromising the security of all parts of previously identified information and communication systems, rank them by the negative impact they may have, and calculate the probability of occurrence;
4. Decide which risks to mitigate and by what measures, what to accept and for which no action should be taken;
5. Make records of identified risks;

6. Prescribe a regular obligation to constantly monitor weaknesses and threats, and to update information on the changes caused by the risk.

OBJECTIVE C: Raising awareness and knowledge on cyber security

In order to achieve all strategic objectives, especially the one related to raising awareness and level of education, it is necessary to take measures to disseminate information on the necessity to protect information and the information and communication infrastructure. These measures will raise the general level of citizens' education in this area, reduce the outflow of professional staff, and increase the number of competent persons who can design and implement protection measures.

C1: Raising cyber security awareness

A prerequisite for implementing any strategy is the support of institutions and decision-makers. Decision- makers need to understand the need to adopt and implement a cyber security strategy. This understanding should be based on being well informed, and understanding the problem being addressed. This does not require technical knowledge of information and communication systems. It is sufficient to be aware that the security of information and information and communication infrastructure can be compromised, which can result in catastrophic consequences, and that there are measures that can reduce the risk of such events. Apart from decision- makers, all persons who come into contact with data considered critical and who work with critical information and communication infrastructure should be aware of the need to protect this data and infrastructure. Cyber security awareness is essential for the adoption and implementation of information security measures at all places, at all levels and in all time frames. A society that achieves a level of general information will be a safer society.

Activities:

1. Regularly inform decision- makers about cyber security, security-relevant past events and their consequences, and possible future consequences of non-enforcement of the measures of protection;
2. Introduce cyber security as a mandatory training program for employees of critical services and databases providers of critical importance, as well as for employees of public administration institutions;
3. Campaign through the media, including social networks, to raise awareness of the need for cyber security;
4. Support the processes of inclusion of media and information literacy in formal and non-formal education.

C2: Strengthening the training and education programs

In addition to raising awareness of all actors on cyber security, it is also important to raise the level of specialised knowledge in this area, both among professionals and within the general population. This can be achieved through formal, non-formal and lifelong learning. Bosnia and Herzegovina needs to increase the number of cyber security experts if it aspires to successfully protect itself against cyber threats. In order to achieve this, it is necessary to introduce studies specialized in this field into schools and Universities in Bosnia and Herzegovina. In addition, regular professional development of all persons responsible for the technical aspects of information security in all institutions at all levels should be introduced. Specialized training, provided by manufacturers, for the use of equipment and software used in an institution, should be mandatory for officials working with them. Apart from the education of cyber security professionals, it is necessary to raise the level of knowledge in this field among citizens. It is a process that needs to be implemented throughout education from primary school to University. In this way, the overall level of knowledge and security of the whole society is raised.

Activities:

1. Introduce specialized studies and cyber security programs at Universities;
2. Introduce mandatory cyber security specialist training to work with platforms used in public administration institutions;
3. Introduce cyber security and media and information literacy topics into curricula of all levels of education.

C3: Encouragement of employment of ICT personnel in the public sector

The proper functioning of information and communication systems, as well as their security, relies on qualified ICT staff. The contemporary job market offers high salaries to these people. Institutions generally have defined pay grades that do not allow the payment of ICT staff at market rates. For this reason, ICT staff goes to private companies or leave the country. It is necessary to find a way to stop this process. This can be accomplished by changes in the way income of skilled ICT staff in institutions is calculated, through additional training opportunities, and a stimulating work environment.

Activities:

1. Adequate evaluation of the work of ICT staff;
2. Provide continuous training for ICT staff;
3. Promote the challenges of working on large information and communication systems.

C4: Research and Development stimulation

Research and development allows for the anticipation and prevention of potential cyber hazards. Research and development should be organized with a focus on cyber security specific to Bosnia and Herzegovina. Research and development requires investment that needs to be planned in the budgets of the institutions and Ministries responsible for science. Academia should co-operate more actively with institutions and the economy. Scientific research and professional projects are the basis of research and development. Efforts should be made to become involved in international projects. In order to achieve quality for inclusion in competitive international projects, it is necessary to first invest in domestic projects through which competences will be developed and papers will be published, consequently having our researchers recognized in the research community. More active participation in scientific and professional conferences should be encouraged. In this way, they exchange experiences and prepare for the challenges ahead.

Activities:

1. Encourage investment in cyber security research;
2. Define specific areas of cyber security that research should focus on;
3. Encourage participation in international cyber security research projects;
4. Encourage researchers' participation in cyber security conferences;
5. Encourage Academia's co-operation with institutions.

OBJECTIVE D: Functional Bodies in charge of Securing, Strengthening and Improving Cyber Security

In order to combat cyber threats in a coordinated manner, it is necessary to have bodies in charge of this. These bodies should have clearly defined competencies that are consistent with the territory and the sector in which they operate. The establishment of these bodies should adhere to international standards and rules, and those of the EU in particular. The NIS Directive imposes obligations on EU Member States in this field, and this Strategic Framework is also aligned with the requirements of the NIS Directive. The competent authorities, the points of contact and the CSIRTs, whose tasks are related to the security of information and communication systems, should be designated.

D1: Designated competent authorities for the security of information and communication systems

It is necessary to have appointed competent authorities in Bosnia and Herzegovina for the security of information and communication systems covering at least the sectors and services listed in Annex I. Competent authorities should have adequate resources to fulfil the assigned responsibilities. Competent authorities, whenever necessary and in accordance with applicable legislation, consult with and co-operate with the competent law enforcement and law enforcement authorities and data protection authorities.

Activities:

1. Identify required bodies and their competencies;
2. Establish competent authorities with adequate human and material resources.

D2: Point of Contact established

It is necessary to establish a point of contact for the security of information and communication systems in accordance with the NIS Directive and the constitutional and legal competences. The Point of Contact performs a liaison function to ensure the international cooperation of competent authorities in Bosnia and Herzegovina with relevant authorities in other countries.

Activities:

1. Establish a point of contact in accordance with the NIS Directive;
2. Provide adequate human and material resources for the point of contact.

D3: Required CSIRTs established

It is necessary to appoint CSIRTs that meet the requirements of Item 1 of Annex III and cover, as a minimum, the sectors and services in Annex I responsible for risk mitigation and the prevention or elimination of incident consequences in accordance with a precisely prescribed procedure. The CSIRT may be established within the competent authority. Appointed CSIRTs should be provided with adequate resources to effectively carry out the tasks set out in Item 2 of Annex III. Effective and secure collaboration of CSIRTs should be facilitated. For communication and information, CSIRTs need access to appropriate, secure and resilient infrastructure.

Activities:

1. Identify required CSIRTs and their competencies;
2. Establish and strengthen the capacities of CSIRTs in human, technical, operational and institutional terms;
3. Establish a suitable, secure and resilient communication infrastructure for CSIRTs.

OBJECTIVE E: Improved Security and Resilience of Information and Communication Systems

In addition to critical information and communication infrastructure, it is necessary to protect public information and communication infrastructure with the providers of key services and databases. The providers of this infrastructure are all holders of licenses issued by the Regulatory Agency of Communications of Bosnia and Herzegovina. These include ISPs, mobile and landline telephony, and network operators. These providers should have a legal obligation to enforce cyber protection of their systems. In order to ensure that protection is enforced, it is necessary to define the minimum protection measures and parameters that control the enforcement of protection. Providers should be obliged to use a neutral internet traffic interchange point (IXP) for traffic between institutions, and to be encouraged to use it for all traffic within BiH. Private providers should be encouraged to invest in cyber protection.

E1: Legally defined obligation to enforce the protection of public information and communication infrastructure for all public and private providers

The Regulatory Agency for Communications, as the body responsible for the holders of licenses for the provision of communications services, should ensure that the providers of communications services have a legal obligation to enforce the cyber protection of their systems.

Activities:

1. Analyse the existing regulation for the protection of public information and communication infrastructure;
2. Prescribe a (legal) obligation to protect public information and communication infrastructure for public and private providers.

E2: Technical supervision of measures of protection of public information and communication system operators and consulting on measures is provided

The Regulatory Agency for Communications should prescribe the security requirements that providers should meet and that can be monitored. These requirements should at a minimum include international cyber security standards that providers should comply with. In addition, it is necessary to regulate the protection of users' privacy, the obligation to inform about security incidents and to co-operate with other providers and law enforcement agencies in incidents.

Activities:

1. Define security- relevant monitoring and control parameters;
2. Provide continuous monitoring of security- relevant parameters;

3. Conduct regular reviews of the work of public information and communication infrastructure providers.

E3: The Neutral Internet Traffic Interchange Point (IXP) is used for traffic between institutions

Using a neutral internet traffic interchange point (IXP) eliminates unnecessary travel of internet traffic between two users in a country, via ISPs from other countries. This reduces data security risks and lowers ISP costs. Bosnia and Herzegovina has one IXP established at the University Tele-Information Centre (UTIC) of the University in Sarajevo, but there may be more in the future. ISPs should undertake to ensure that traffic between institutions in Bosnia and Herzegovina using different ISPs exclusively travels through the IXP and never outside the country. The exception to this rule is the traffic to the approved *cloud computing* providers that these institutions use. It is generally more efficient and cost effective for ISPs to use IXP for all their users, not just institutions, and this should be encouraged.

Activities:

1. Require ISPs of the institutions to direct traffic to institutions other than their users exclusively through IXP, except for traffic to approved *cloud computing* service providers outside of Bosnia and Herzegovina.

E4: A safe way to use *cloud computing* is defined

Cloud computing enables the rational and economical use of computing resources. In the case of *cloud computing*, data is sent and processed outside the organization that owns it. The place of processing may be in another country. This raises the question of enforcing the security of such data and responsibilities. Only *cloud computing* providers certified to meet international security standards, especially those related to *cloud* security, should be used to provide the required level of security. Examples of such standards are the ISO 27000 family of standards, and ISO27017 in particular focused on the *cloud*. It is necessary to consider whether there is data that should not be sent to the *cloud* or to the *cloud* outside of Bosnia and Herzegovina. Such data should be defined and ensured that they are not used by the *cloud*, i.e. *cloud* outside Bosnia and Herzegovina.

Activities:

1. Define a minimum set of security standards that *cloud computing* providers should meet;
2. Only use *cloud computing* providers that meet the established standards;
3. Consider whether there is data that should not be sent to the *cloud* at all or should not be transmitted to the *cloud* outside of Bosnia and Herzegovina, and if so, to identify which are those;

4. For data for which it is determined to be inadmissible, enforce the prevention of sending to the *cloud* or to the *cloud* outside of Bosnia and Herzegovina.

E5: Private information and communication sector encouraged to invest in security measures

Private providers should ensure that their investments are economically viable. Although cyber security investments pay off in the long run, initial investments can be too big of a short-term financial burden. For this reason, it is necessary to find appropriate ways to encourage private providers for these investments. This may be through certain reliefs for necessary procurement designed to increase cyber security. It would be desirable to set up research funds and cyber security centres to assist private providers. Capacity needs to be developed to assist private providers in security incidents. This should include assistance with data recovery and forensic analysis of the incident.

Activities:

1. Consider introducing benefits for communication service providers for the cyber security investments;
2. Enable private communications service providers to access publicly funded cyber security research results;
3. Provide support to communications service providers following cyber incidents.

OBJECTIVE F: Enhanced Capacity to Combat Cybercrime

The constant improvement and increase in sophistication of cybercrime and cyber-enabled crime, as well as the methods and techniques by which cybercrime is carried out, requires continuous capacity building in order to respond effectively to cybercrime. Cybercrime and electronic evidence require specialized response from law enforcement institutions. These institutions and the justice system should be able to investigate and prosecute cybercrime and cyber- enabled crime, and use electronic evidence relating to any crime. Cybercrime and cyber- enabled crime should be adequately addressed in legislation. Law enforcement institutions should have adequate human and material resources. Prosecutors' Offices and Courts should be aware and adequately trained in contemporary cybercrime.

F1: Constant development of legislation in the area of cybercrime and cyber –enabled crime.

New types of criminal offenses are emerging along with the rapid technological development,. Different forms of cybercrime may be unrecognized in the legislation. This opens for the possibility that some acts may not receive a legal qualification. The competent law enforcement institutions and

the judicial system then have no basis for taking action to prevent these acts and to sanction the perpetrators. For this reason, it is necessary to regularly monitor new outbreaks of cybercrime and cyber- enabled crime, and analyse whether existing legislation recognizes them. If not, the law needs to be amended. As laws change more slowly than new forms of cybercrime appear, it is necessary to consult with experts when amending the laws covering this area.

The activities pursued by the foregoing are as follows:

1. Regularly analyse the compliance of existing legislation with contemporary forms of cybercrime;
2. Develop legislation in line with the results of analyses.

F2: Developed human and technical capacities of law enforcement institutions

The rapid development of technology enables new forms of crime. In order to combat these forms of crime, it is necessary to have adequately educated staff in law enforcement institutions. This education should be continuous and include both technical and criminal aspects. Trained personnel are needed, but not sufficient on their own. It is necessary to technically equip law enforcement institutions with the equipment and software needed to prevent, detect and process cybercrime. Law enforcement institutions should have specialised teams to combat cybercrime.

Activities:

1. Regularly educate employees of cybercrime law enforcement agencies and its forensics;
2. Technically equip law enforcement institutions with the necessary equipment to combat cybercrime;
3. Improve digital forensics capacity;
4. Establish and strengthen specialized cybercrime teams in all relevant law enforcement institutions, in accordance with strategic assessment and needs identified;
5. Establish special cybercrime departments or, in systematization, anticipate prosecutor(s) and judge(s) for cybercrime in competent Prosecutors' Offices and Courts.

F3: Continuous training of prosecutors and judges on contemporary cybercrime

Prosecutors and judges need to be aware of the contemporary forms of cybercrime and cyber-enabled crime. They need to be regularly briefed and trained on the characteristics of cybercrime that are different from classic crimes. Prosecutors and judges need to know the characteristics and specifics of electronic evidence. They need to understand the importance of collecting this evidence in a timely manner and their sensitivity to change. Prosecutors need this knowledge to adequately conduct

cybercrime investigations, and for judges to facilitate the presentation and evaluation of electronic evidence in cybercrime cases.

Activities:

1. Regularly train prosecutors and judges on contemporary cybercrime;
2. Regularly train prosecutors and judges on electronic evidence.

OBJECTIVE G: Effective Cyber Security Co-operation Established in International, Regional and Domestic Frameworks

Cyber security should be implemented comprehensively in order to be successful. It is necessary to establish effective cooperation across sectors and at all levels, from local to international. This cooperation should be consistent with the competencies. Co-operation mechanisms should be in line with the requirements of the NIS Directive.

G1: Effective domestic cyber security co-operation achieved

Co-operation and exchange of the necessary information between the Point of Contact, the competent authorities and the CSIRTs should be ensured. Effective, efficient and secure co-operation of all CSIRTs, regardless of sector and territory, should be ensured.

Activities:

1. Ensure the provision of security incident information to the responsible CSIRTs;
2. Provide CSIRTs with access to the information necessary to perform their tasks with key service providers in accordance with their responsibilities;
3. Ensure the exchange of relevant information between CSIRTs and the Point of Contact;
4. Ensure effective, efficient and secure collaboration of all domestic CSIRTs.

G2: Engaging in international and regional co-operation

International and regional co-operation enables the exchange of information on current security-related developments in the area of ICT, as well as in other areas. This supports timely and up-to-date preparation and response to possible attacks. Through this collaboration, knowledge sharing is enabled and a knowledge base is created that strengthens all participants in the exchange. Engaging in international co-operation means adopting and implementing international cyber security standards. International co-operation facilitates research and development, which contributes to increasing the cyber security knowledge. The membership of Bosnia and Herzegovina in the UN, OSCE, the Council of Europe, FIRST, TF-CSIRT and others imposes obligations on the implementation of the adopted cyber security measures. Fulfilling these obligations brings access to the resources of these

organizations. The minimum form of international cooperation that must be ensured is the exchange of information with other countries and international organizations through a Point of Contact.

Activities:

1. Strengthen and broaden co-operation of Bosnia and Herzegovina with international partners within organizations of which Bosnia and Herzegovina is a member, such as the OSCE, the Council of Europe and the UN, and organizations whose aspirations are sought, above all the EU, and co-operation with countries in the region in particular;
2. Participate in and organize international practical and theoretical knowledge sharing such as cyber security exercises, trainings, conferences and seminars;
3. Ensure adequate exchange of information with other countries and international organizations.

OBJECTIVE H: Capacity Built to Adequately Respond to Crisis

Experience has shown that, in spite of all preventive measures for cyber security protection, situations can occur where the functioning of the critical information and communication infrastructure, and thus the provision of key services, may be endangered. Such situations require preparation in order to reduce their negative impact and end it as quickly as possible. Preparations consist of identifying behavioural procedures and providing the necessary resources for response. First of all, it is necessary to define precisely what is considered a crisis to allow for its identification and notification in accordance with a procedure that should also be defined. Crisis reporting should set in motion the prepared procedures and operational plans with all relevant actors. As the primary means of communication may be affected by a crisis incident, alternative communication channels need to be prepared in advance. In order to achieve this, it is necessary to have adequate human and material resources that can implement the planned measures.

H1: Criteria for crisis identification established

Competent authorities should prescribe criteria for crisis identification to the key services and databases providers. The basic criteria that should be used to evaluate how much an incident is a crisis are: the number of users for whom the incident caused the key service to be interrupted; the duration of the incident; the geographical size of the areas that could be affected by the incident; the extent of service disruption and the extent of the impact on economic and social activities.

Activities:

1. Establish crisis criteria for all key service providers and databases.

H2: Reporting Incidents Mechanisms established

Key services and databases providers are required to report immediately to the competent CSIRT all security incidents on critical information and communication infrastructure. The competent CSIRT is to assess the severity of the incident and take further action based on that assessment. The competent CSIRT may, if it deems necessary, forward the incident information to other CISRTs or Point of Contact, and may issue a security alert. Security alerts can be public to all citizens and institutions or targeted at a law enforcement authority or institution.

Activities:

1. Require key service and databases providers to report incidents on critical information and communications infrastructure to the competent CSIRT;
2. Advise key service and database providers to report other incidents to the responsible CSIRT;
3. Establish an incident severity assessment procedure in CSIRTs;
4. Establish a procedure for issuing security alerts;
5. Establish an alternative communication infrastructure in cyber incidents cases.

H3: Developed operational plans and procedures for crisis management for all responsible institutions

All key service and database providers, all CSIRTs, all competent authorities and the Point of Contact should establish procedures and operational plans defining how crisis behaviours and actions are handled. These procedures and plans may include other institutions, such as competent Ministries or Regulators, who also should have their own crisis management procedures and plans within their jurisdiction. There is also a need to have a procedure and authority to communicate with the public in these situations. Procedures and operational plans should be tested, preferably through simulation of cyber attacks, and based on the results, have it analysed and updated.

Activities:

1. Develop crisis procedures and operational plans in all key services and database providers, CSIRTs, competent authorities and the Point of Contact, with the necessary degree of harmonization;
2. Define the institutions which, in addition to the above, should be included and which should draw up procedures and plans;

3. Determine the competence and manner of communication with the public in crisis situations;
4. Conduct regular and joint cyber-attack simulations to verify procedures and operational plans;
5. Update crisis procedures and operational plans at least annually, and if necessary, after cyber-attack simulations.
6. Encourage the establishment and development of crisis management centres

H4: Personnel and resources filled organizations in accordance with crisis plans and procedures

Pursuant to the established crisis procedures and plans, it is necessary to train responsible staff and provide other necessary resources for implementation of the procedures and plans.

Activities:

1. Train staff in accordance with the crisis procedures and operational plans;
2. Provide necessary resources to implement crisis procedures and operational plans

OBJECTIVE I: Public - Private Partnership Established

The private sector - companies and privately owned corporations - is an essential element in the cyber security sector. Effective and clearly defined co-operation and strategic partnerships on cyber security issues need to be established with these companies for mutual benefit. The European legislation[9] encourages the need for public- private co-operation in the area of cyber security and the importance of building trust through public-private partnerships (PPPs)[10]. In this regard, ENISA has published the document "PPP: Collaboration Models"[11], which develops in detail the recommended and successful PPP models and identifies successful existing solutions for their application within the European Union.

Public- private partnerships in terms of industrial and academic development and innovation are also a form of necessary and possible co-operation. An example of this is the comprehensive PPP agreement signed between the European Union and the European Cyber Security Organization network (ESO)[12].

[9] „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace and Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU“
[10] OECD defines PPP as "An arrangement in which the private sector offers infrastructure goods and services traditionally provided by state governments." https://stats.oecd.org/glossary/detail.asp?ID=7315

[11] https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
[12] https://www.ecs-org.eu/documents/contract.pdf

I1: Established public- private partnership with companies and corporations that develop and offer cyber security products, solutions and services

Private companies develop, market and implement all products (software and hardware) as well as solutions for protecting IT systems and data. Also, private companies and corporations develop and market the cyber security services, whether as integrated services, consulting or both. In addition, a part of the key services providers are private companies. In addition to the large global corporations that successfully provide these services to institutions, corporations and governments around the world, such expertise is being developed in the private sector through global partnerships and services such as Managed Security Service Provider (MSSP). Private sector knowledge, resources and technical capabilities can be made available to other public and private organizations on a permanent basis or when the need arises, especially in times of crisis.

Activities:

1. Establish strategic collaboration and establish channels and frameworks for collaboration with global manufacturers and providers of cyber security products, solutions and services;
2. Establish direct co-operation and strategic partnerships with domestic companies offering products, solutions and services in the area of cyber security, with the aim of establishing appropriate expertise, personnel base and technical resources within Bosnia and Herzegovina;
3. Establish a form of direct collaboration, public- private partnerships - PPPs with providers, primarily global corporations in the cyber security services sector, which could be urgently activated in case of need and crisis. Review the expertise of key service providers.

I2: Public-private partnership with key service providers established

Privately owned key services providers are subject to the obligation to protect their critical information and communication infrastructure in accordance with the regulations of the Regulator and the applicable sector-specific legislation. These providers should not only had imposed obligations but also be provided with support in enforcing security. It is possible to rationally use limited human resources with well-organized co-operation. Knowledge and technical skills existing in an organization, public or private, can be made available to other organizations in the sector or beyond, when the need arises, especially in crisis.

Activities:

1. In co-operation with the competent regulatory authorities, define precisely the obligations of the private sector to secure critical information and communication infrastructure, and to provide appropriate control mechanisms;

2. Review the expertise of key service providers;
3. Encourage mutual professional support and exchange of information among key service providers within the sector and, where appropriate, beyond.

I3: A public- private partnership for the exchange of information has been established

Exchange of information on cyber security events between all organizations, public and private, enables timely and adequate response to them. It is necessary to have in place mechanisms of exchange and protection of both, the classified information between domestic and foreign private companies, and corporations and the public sector in BiH. It is necessary to ensure that all parties involved can actively participate in the exchange of information in accordance with the law.

Activities:

1. Private and public companies, in accordance with the needs of classified information exchange, will establish mechanisms for the exchange and protection of classified information by obtaining Facility Security Clearances issued by the National Security Authority.

III. Concluding considerations

The Strategic Framework is an initial step towards building a more secure society in cyber space. This document presents guidelines for harmonizing the existing and developing the future cyber security strategies in BiH, through specific activities outlined in the description of each of the objectives, and facilitates the development of Strategies and Action Plans. Action plans need to define the institutions responsible for implementing the activities in line with competencies, as well as deadlines, required resources and performance indicators.

The success of implementing activities from the Strategic Framework through Strategies and Action Plans depends on many factors. Based on the experiences of countries that have gone through this process, ENISA[9] has identified the following most common challenges and aggravating circumstances:

- **Establishing successful co-operation between institutions**

  It may be difficult to answer and resolve the issue of cyber security competency and responsibility. This leads to the waste of resources for multiple protections against the same risk or the complete non-coverage of some risk. The solution lies in the well-established structure and co-operation of bodies responsible for securing, strengthening and improving cyber security.
- **Establishing trust between the public and private sectors**

  The private sector should believe that investment in cyber security, especially if imposed through regulations, actually helps its business to thrive. Then the private sector will accept these investments as a business need, not an unnecessary expense. The public sector should believe that the money invested in enhancing the security of the private sector contributes to the security of the entire society without being superfluous from budgeting.
- **Provision of appropriate resources**

  Investment is required to achieve the goals. With cyber security, problems are often not material, but problems are human resources. Building the requisite professional staff is a process that cannot be completed in a short time and therefore the process should start immediately. Of course, adequate financial resources are also necessary for the development of human resources and for the procurement of equipment.
- **Promoting a shared approach and raising awareness about data protection and privacy**

  The lack of a common approach among all actors to protect cyber security leads to disparate and inefficient action. There is a need for active awareness-raising, especially for concerted action. The issue of privacy and data protection often comes up as very complex for a balanced approach.

- **Conducting security vulnerability and risk analysis**

  This analysis can be very demanding and difficult to carry out if the requirements are made too broad. A focused approach in smaller areas is preferred, which will result in a more accurate and less comprehensive risk analysis, the results of which can be directly used to implement concrete measures.

A popular phrase from cyber security says that security is a process, not a product or condition. For this reason, strategic documents are not documents that are written once and used forever. The strategic documents need to be evaluated on a regular basis for periods not exceeding those stated in the vision, which in this case is five years. The evaluation should be done by an independent body from the one who wrote or implemented the Strategic Framework. Resources are needed for evaluation. The evaluation assesses the degree of fulfilment of global goals, as well as the realization and success of individual activities. Good and bad practices need to be identified from the process of implementing the Strategic Framework. The strategic framework is updated based on the results of the evaluation as well as the review of the cyber security situation. The update includes changes to global goals and individual activities. In order to facilitate and objectify the evaluation process, it is necessary to define the Key Performance Indicators (KPIs) of the implementation of the strategic framework. For each of the global goals, on the basis of the planned activities, concrete and measurable quantities are determined, which show the extent to which the planned activity was achieved and how much it contributed to the achievement of the global goal.

- The relevant documents used in the preparation of the Guidelines are as follow:
  1. OSCE DECISION No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From The Use of Information and Communication Technologies; PC.DEC/1202, of 10 March 2016; available at: https://www.osce.org/pc/227281?download=true
  2. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Security for Network and Information Systems across the Union (NIS Directive)
  3. NCSS Good Practice Guide- Designing and Implementing National Cyber Security Strategies, 2016.
  4. Guide to Developing a National Cybersecurity Strategy, ITU, 2018.
  5. Convention on Cybercrime, Budapest, 23 November 2001, came into force on 01 July 2004, came into force in relation to BiH on 01 September 2006; published in the "Official Gazette of BiH" – International Treaties number: 06/2006);
  6. Additional Protocol on the Convention on Cybercrime, Concerning the Criminalisation of Acts a Racist and Xenophobic Nature Committed through Computers Systems, Strasbourg,

28 January 2003, came into force on 01 March 2006, came into force in relation to BiH on 01September 2006; published in the "Official Gazette of BiH" – International Treaties number: 06/2006);

7. Report on the Results of the RAC Annual Survey of Users licenses for Providing Internet Services in Bosnia and Herzegovina for 2018 - estimates that in 2018 there were 3,195,294 Internet users, i.e. the Internet usage rate in Bosnia and Herzegovina for 2018 is 90,49%. Available at: https://docs.rak.ba//documents/ea9d822c-b1dc-4ad9-b2d9-735dc6c8ea91.pdf
8. DIRECTIVE (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on o the protection of individuals with regard to the processing of personal data and the free movement of such data, and the repeal of the Directive 95/46/EU (General Data Protection Regulation); Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679
9. CYBERSECURITY CAPACITY REVIEW, Bosnia and Herzegovina, Global Cyber Security Capacity Centre, March 2019
10. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, OSCE, 2013
11. Cyber Security Strategy - Establishment of a High Cyber Security Assurance System in the Ministry of Defence and Armed Forces of Bosnia and Herzegovina, 2017
12. Developing a National Strategy for Cybersecurity - Foundations for Security, Growth, and Innovation, Microsoft, 2013.
13. National strategy for the protection of Switzerland against cyber risks, 2012
14. Finland´s Cyber security Strategy, 2013
15. National Cyber Security Strategy, Spain, 2013
16. Decision on Adopting the National Cyber Security Strategy and Action Plan for the Implementation of the National Cyber Security Strategy, Croatia, 2015
17. Strategy for the Development of Information Security in the Republic of Serbia for the Period from 2017 to 2020, 2017.
18. Cyber Security Strategy of Montenegro 2018-2021, 2017.
19. National Cyber Security Strategy 2016-2021, UK, 2016.
20. National Cyber Security Strategy 2, From awareness to capability, Netherlands, 2018.
21. A national cyber security strategy, Sweden, 2017.
22. National Cyber Security Strategy, of the United States of America, 2018.

ANNEX I - REQUIRED KEY SERVICES SECTORS UNDER NIS DIRECTIVE

1. Energetics
    a. electricity
    b. oil
    c. gas
2. Transport
    d. air
    e. rail
    f. aqueous
    g. road
3. Banking
4. Financial market infrastructure
5. Health services
6. Water-supply
7. Digital infrastructure

Mandatory digital services (NIS Directive Annex III)

1. Internet market
2. Internet browser
3. *Cloud computing* services

ANNEX II - KEY SERVICE PROVIDERS UNDER NIS DIRECTIVE

1. **Energetics**
   a. electricity
   - Electricity and Energy Companies performing at least one of the following functions: generation, transmission, distribution, supply or procurement of electricity, and which are responsible for the commercial, technical or maintenance tasks associated with those functions
   - Transmission and distribution system providers for electricity

   b. oil
   - Oil pipeline operators
   - Operators of oil production, oil refineries and oil plants and its storage and transfer

   c. gas
   - Gas supply companies
   - Gas Distribution System Operators
   - Gas Transmission System Operators
   - Gas storage system operators
   - Liquefied natural gas terminal operators
   - Natural gas companies
   - Operators of natural gas refining and treatment plants

2. **Transport**
   a. Air
   - Air carriers
   - Airport managing body and airport, and bodies managing ancillary facilities at airports
   - Air traffic control operators providing air traffic control services

   b. Rail
   - Rail Infrastructure Managers
   - Rail transportation companies, including service facility operators

   c. Aqueous
   - Inland waterway, sea and coastal passengers companies, inland waterway and sea freight shipping companies, not including individual vessels operated by those companies
   - Port managing bodies, including their ports, and entities managing facilities and equipment in ports
   - Maritime Traffic Control and Management Service

   d. Road
   - Road authorities responsible for traffic management
   - Operators of intelligent traffic systems

3. **Banking**
   - Loan institutions

4. **Financial Market Infrastructure**
   - Trading venue operators
   - Central Contracting Parties (text taken over from 648/2012 Article 2, paragraph 1)

5. **Health System**
   - Health Care providers

6. **Water-supply**
   - Suppliers and distributors of water intended for human consumption but excluding distributors to whom the distribution of water for human consumption forms only a part of their general activity of distributing other goods and products, which are not considered essential services

7. **Digital infrastructure**
   - IXPs
   - DNS service providers
   - TLDs name register

ANNEX III - REQUIREMENTS REGARDING THE COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) AND THEIR TASKS UNDER THE NIS DIRECTIVE

1. Requirements regarding CSIRTs:

    a. CSIRTs ensure a high level of availability of their communications services by avoiding unique breakpoints and have several resources available at all times for two-way contact. Furthermore, communication channels are clearly defined and well known to clients and associates.
    b. CSIRT premises and support information systems are located in secure locations.
    c. Continuity of work:
        i. CSIRTs are equipped with an appropriate request management and redirection system to facilitate handovers.
        ii. CSIRTs have enough qualified employees to ensure availability at all times.
        iii. CSIRTs rely on infrastructure whose continuity is assured. For this purpose redundant systems and spare workspace are available.
    d. CSIRTs have the opportunity, if they wish, to participate in international cooperation networks.

2. CSIRTs Tasks:

    a. The tasks of CSIRTs cover at least:
        i. incident tracking;
        ii. providing early warnings and announcements and informing relevant participants of risks and incidents;
        iii. responding to incidents;
        iv. providing dynamic risk and incident analysis and situation review;
        v. participating in a network of CSIRTs.
    b. CSIRTs establish co-operation with the private sector.
    c. With the aim of facilitating co-operation, CSIRTs promote the adoption and implementation of common or normative practices for:
        i. incident and risk management procedures;
        ii. plans for the classification of incidents, risks and information.

ANNEX IV - DEFINITIONS and ABBREVIATIONS

CERT- Computer Emergency Response Team

Cloud computing - a digital service that provides access to an upgradable and resilient set of shared computing resources.

CSIRT- Computer Security Incident Response Team

Cyber - refers to people, things, policies, concepts and ideas related to computer devices and computer networks, and in particular the Internet and information technologies.

Cybercrime - criminal activities in which the information and communication systems are the object, means, target or place of the crime.

Cyber space - more than the Internet, it involves not only hardware, software and information systems, but also people and social interaction within these networks.

DNS service provider - entity providing DNS (Domain Name System) services on the Internet

DNS- Domain Name System

ENISA- European Network and Information Security Agency

EU – European Union

Facility Security Clearance - industrial security authorizations

FIRST- Forum for Incident Response and Security Teams

GDPR – (*General Data Protection Regulation*) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation)

GEANT – a pan-European computer network for the research and education community

ICT – Information and Communication Technology

Incident - any event that has a real adverse effect on the security of information and communication systems;

Information and Communication System

a. any device or group of connected or related devices, one or more of which programmatically performs automatic processing of digital data;

b. digital data stored, processed, retrieved or transmitted by the elements described in "a." for the purpose of operation, use, protection and maintenance thereof;

Information security - a state of confidentiality, integrity and availability of information

Internet browser - a digital service that allows a user to perform searches, in principle, on all web pages or web pages in a specific language based on a query, on any topic, in the form of a keyword, sentence or other entry, resulting in *links* where to find information that is related to the content requested;

Internet market - a digital service that enables consumers and / or merchants to enter into purchase and service contracts with merchants on the Internet on the website of that Internet market or on the website of that merchant using computer services provided by the Internet market;

ISO- International Organization for Standardization

ISP- Internet Service Provider

ITU- International Telecommunication Union

IXP- Internet Exchange Point

PPP- Public- Private Partnership

Key Service - a service essential to the maintenance of key social and/ or economic activities, and at a minimum the services defined in the Annex I

KPI- Key Performance Indicator

Critical information and communication infrastructure – the information and communication infrastructure of the key service provider necessary to provide that key service

Crisis - a situation in which the functioning of the critical information and communication infrastructure is compromised and thus the provision of key services;

MSSP-Managed Security Service Provider

Neutral point for internet traffic exchange (IXP) - a network instrument that enables the interconnection of two or more independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic; IXP provides interconnection for autonomous systems only;

NIS Directive – (Network and Information Security) 2. DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Security for Network and Information Systems across the Union (NIS Directive)

NIST- National Institute of Standards and Technology

Key Service Provider - a public or private entity of the type listed in Annex II that provides one of the key services

OSCE – Organization for Security and Co-operation in Europe

Top- Level Domain Register - an entity that manages and handles the registration of Internet domain names for a specific supreme domain (TLD);

Risk - any reasonably identifiable circumstance or event that has a potential adverse effect on the security of information and communication systems;

Information and Communication System Security - the ability of information and communication systems to resist, at a certain level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or related services that these information and communication systems offer or provide access to;

Domain Name System - a hierarchically distributed online naming system that answers queries about domain names;

TLD- Top-level Domain

TF-CSIRT (*Task Force Computer Security Incident Response Teams*) – GEANT Task Force for CSIRTs

UN – United Nations

ANNEX V – GENERAL OVERVIEW OF THE EXISTING INTERNATIONAL COMMITMENTS, POLICIES, STRATEGIES, LAWS AND REGULATIONS RELATING TO CYBER SECURITY IN BOSNIA AND HERZEGOVINA

International Commitments :

A series of UN General Assembly resolutions on cyber security

OSCE Confidence Building Measures to Reduce The Risks of Conflict Stemming From The Use of Information And Communication Technologies

European Union Cyber Security Strategy

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Security for Network and Information Systems across the Union (NIS Directive)

Council of Europe Convention on Cybercrime / Budapest Convention

International Telecommunications Regulations

EU (Commission)Digital Agenda for the Western Balkans

Stability Pact – e-Southeast Europe initiative –

Policies:

Information Society Development Policy for the period 2017-2021 (link page 19, column III – Encouraging Confidence and Security Building) ("BiH Official Gazette" No. 42/17) of Bosnia and Herzegovina

Strategies:

Strategic Plan of the Ministry of Security of Bosnia and Herzegovina for 2017-2019,

Strategy for Combating Terrorism in Bosnia and Herzegovina 2015-2020

Strategy for the Fight against Organized Crime in Bosnia and Herzegovina 2017-2020

Action Plan for the Protection of Children and Prevention of Violence against Children Committed through ICT in Bosnia and Herzegovina

Cyber Security Strategy of the Ministry of Defence of Bosnia and Herzegovina

Cyber Security Action Plan of the Ministry of Defence of BiH

Legislation:

Law on Information Security of Republika Srpska ("Official Gazette of RS" number 70/11)

Law on Critical Infrastructure Security of Republika Srpska ("Official Gazette of RS" number 58/19)

ANNEX VI - INSTITUTIONS, BODIES AND OBSERVERS, MEMBERS OF THE INFORMAL WORKING GROUP WHO CONTRIBUTED TO THE DEVELOPMENT OF THE GUIDELINES FOR A STRATEGIC CYBERSECURITY FRAMEWORK IN BOSNIA AND HERZEGOVINA UNDER AUSPICES OF THE OSCE MISSION TO BIH

Observers
International Organizations and Diplomatic Missions:

1. Mr. Mak Kamenica, USAID Deputy Director, Energy Investment Activities,
2. Mr. Milan Sekuloski, Europe and Central Asia Senior Advisor, DCAF- Geneva Centre for Security Sector Governance
3. Ms. Irina Rizmal, Project Assistant, DCAF- Geneva Centre for Security Sector Governance,
4. Mr. Adel Abusara, Senior Project Assistant, Democratic Governance, OSCE Mission to Serbia

Academia:

1. Mr. Saša Mrdović, Professor, Department of Computer Science and Informatics, Faculty of Electrical Engineering, University of Sarajevo,
2. Mr. Emir Vajzović, PhD, Assistant Professor, Head of Institute for Social Sciences Research, Faculty of Political Science, University of Sarajevo

Council of Ministers of Bosnia and Herzegovina:

3. Ms. Ivana Šarić, Head of Section for Maintenance and Development of e-Government, General Secretariat of the Council of Ministers
4. Mr. Ivan Brčić, Senior Associate, Maintenance and Development of e-Government, General Secretariat of the Council of Ministers

Ministry of Defence of Bosnia and Herzegovina:

5. Mr. Belmir Agić, Assistant Minister, Sector K4UI, Ministry of Defence of Bosnia and Herzegovina

Ministry of Foreign Affairs of Bosnia and Herzegovina:

6. Ms. Stela Šunjić, Minister- Councillor, Head of the Communication and IT Department,
7. Mr. Mirza Pašić, Expert Advisor, Department for OSCE, CoE and Regional Initiatives

Ministry of Security of Bosnia and Herzegovina:

8. Mr. Mate Miletić, Assistant Minister, Sector for Protection of Secret Data
9. Mr. Adnan Kulovac, Head of IT Security Section
10. Mr. Mustafa Arifović, Expert Adviser for IT, Directorate for Coordination of Police Bodies in BiH
11. Mr. Željko Dugonjić, Expert Advisor

Ministry of Communication and Transport of Bosnia and Herzegovina:

12. Mr. Branislav Zimonjić, Senior Expert Associate for IT
13. Ms. Irida Varatanović, Advisor to the Minister
14. Mr. Damir Prlja, MAP REA BiH Contact Person for Digital Integrations

State Investigation and Protection Agency (SIPA):

15. Mr. Alis Gabeljić, Investigator, Criminal Investigation Department, State Investigation and Protection Agency,

Intelligence and Security Agency (OSA/OBA):

16. Mr. Nermin Mehić, Head of Section for IT

Ministry of Foreign Trade and Economic Relations of Bosnia and Herzegovina:

17. Ms. Vera Vitomir, Department for Energy Sector, Energy Sector

Energy Sector:

18. Mr. Edin Zametica, MSci., Secretary General, State Electricity Regulatory Commission (DERK)
19. Ms. Amra Omeragić, Advisor to the General Manager, Elektroprenos BiH
20. Mr. Darko Sinanović, Head of the Information and Telecommunication System Service Independent Systems Operator (NOS) in Bosnia and Herzegovina
21. Ms. Emina Kreštalica,Software Development Engineer, Elektroprivreda BiH, Sarajevo
22. Mr. Jasmin Heljić, Software Development Engineer, Elektroprivreda BiH, Sarajevo

Regulatory Agency for Communications BiH:

23. Mr. Aleksandar Mastilović, Expert Adviser to the Director General, Regulatory Agency for Communications
24. Mr. Predrag Divljan, Head of IT Support Department, Regulatory Agency for Communications

Private Sector:

25. Mr. Enes Haračić, Director, Results Consulting

Government of Federation of Bosnia and Herzegovina:

26. Mr. Adi Kantardžić, IT Sector, General Secretariat of the Government of Federation of BiH
27. Mr. Adis Omerović, Member of the Working Group on ICIS Project

Ministry of Interior of Republika Srpska:

28. Mr. Dragan Grmuša, Head of the Strategic Planning Department, Cabinet of the Minister
29. Ms. Divna Lovrić, Head of ICT Administration
30. Mr. Gojko Pavlović, PhD, International Co-operation Department, Cabinet of the Minister
31. Mr. Olivije Zimonja, Chief of the High Tech Crime Department, Crime Police Administrattion

Ministry of Science and Technology Development, Higher Education and Information Society of Republika Srpska:

32. Mr. Aleksandar Đurić, CERT of Republika Srpska

Ministry of Interior of Federation of BiH:

33. Mr. Nedžad Ćatić, Head of Section for Combating Computer Crime
34. Mr. Saša Petrović, Inspector, Federal Crime Police Investigation Service

Police of Brčko District of Bosnia and Herzegovina:

35. Mr. Neđo Lazarević, Investigator in Crime Police Unit

European Union Delegation to BiH and European Union Special Representative in BiH

36. Mr. Šadi Matar, Political Advisor, Information Society and Media

OSCE Mission to Bosnia and Herzegovina

37. Mr. Bojan Janković, Programme Co-ordinator, Department for Security Co-operation
38. Ms. Sanja Ćatibović, National Programme Officer, Focal Point on Cyber Security