Information & Security: An International Journal

Vesna Poposka, v.34:1, 2016, 25-36 https://doi.org/10.11610/isij.3402

THE URGE FOR COMPREHENSIVE CYBER SECURITY STRATEGIES IN THE WESTERN BALKANS

Vesna POPOSKA

Abstract: The following policy brief aims to allocate the grassroots of cyber security awareness for Western Balkan states through analysis of the legal and policy frameworks in each of the states in the region. The topic is considered as one of the utmost priorities for the region due to (geo-) political, economic and security reasons. The legal and policy frameworks came out to be unclear, and a screening process had to be conducted for this analysis, due to the fact that comprehensive information is lacking, or at least are not publicly available. The first lesson to come out from this cluttered situation points to the need to prepare national cyber security strategies and organise the regional cooperation in that process.

Keywords: cyber security, awareness, strategy, policy, Western Balkans, law.

Introduction

The whole concept of cyber security in the region of Western Balkans is pretty uncommon. The region has faced painful transition to democracy, holding up different priorities that are in fact rather distanced from the cyber security understanding. Albania, Bosnia and Herzegovina, Kosovo, Macedonia, Montenegro, and Serbia have all gone through thorny roads to stabilization. All of the countries of the Western Balkan region are dealing up with the same problems, challenges and aspirations for most of the time. Due to this fact, they are sharing the same risks and same needs, both internally and externally.

Internally, the region has a long history of inner conflicts and international presence and interference. The long period of democratic transition was fatiguing for the markets and the people that also led to ethicizing of social conflicts. Presence of fundamental radical Islam on the Balkans has also been raised as an issue during the last decade. All of Western Balkan countries are dealing up with more or less the same challenges and chasing up more or less the same dreams of Euroatlantic integration. However, they have rarely managed to learn from each other's experience, continuing with and repeating the same mistakes and the same habits. Some countries make neighbours out of the enemies – and that's how the idea of the European integration was born more than a half century ago. Some countries make enemies out of their neighbours – and that recidivism has to be worked out through economic cooperation, based on the European model. The same goes for the issues of cyber security as it is understood in its broadest sense. A Glossary of Common Cyber security Terminology (NICCS, 2014) gives two definitions of cyber security: narrow one, that defines cyber security as "The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation";[1] and extended definition that refers to cyber security as a "Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[1]

Externally, all countries of the Western Balkan region are NATO and/or EU aspiration countries. Albania is a full NATO member, whereas Macedonia is a troop contributor to the international military presence in Afghanistan. This made the region a potential target.

NATO's latest priority is cyber security itself. Both the revised NATO Policy on Cyber Defence of 8 June 2011 and The Chicago Summit Declaration of May 2012 stressed the importance of cooperation with partner nations in order to achieve greater cyber security. The European Commission, in its press release from June 20, 2014 dedicated on Europe's future security challenges, announced that "The growing trend of Europeans fighting abroad in groups affiliated with terrorism, the diversification of international organized crime, and the increased risk of large-scale cyber attacks"[2] are some of the greatest challenges faced.

Although small Balkan countries have tried (and managed to!) and are catching up with the steps necessary for successful Euroatlantic integration, it was not a completely successful move when it comes to cyber security.

The following article aims to provide screening of the current factual situation on cyber security issues in the region, and screening over the international legal and policy framework. Both issues have its own flaws, but they are both essential for preparation of effective cyber security strategy\ as a cornerstone of further activity. In the author's view, cooperation is important for moving from the first (regional) issue to the second (international) as the second represents the framework of best practices to be implemented.

Cyber Security Screening for the Western Balkans: Where Do We Stand?

The first idea and inspiration for the author were a few academic events hosted in Skopje, Pristina, and Petnica, and dedicated to cyber security. The first impression was that for a first time, a region that has gone through crisis and security incidents can gather together and discuss a matter of security that is common and shared, but completely insensitive for the participants. This was essential incentive and academic provocation. I tried to allocate more resources on the topic and harvest the necessary information through official websites and documents. Unfortunately, this operation was not successful for most of the cases. Such situations send a strong clarifying message to any researcher about the position and prioritization that is given to cyber security issues, but also speaks about the average level of understanding and awareness of the issue. Some of the information was controversial or confusing, which made it difficult for the author to extract clear conclusions out of the available data.

For this reason, the author prepared a short questionnaire that was distributed to alumni of cyber security winter school (DCAF Young Faces Network Winter School of cyber security held in Petnica, Serbia, in November 2014) that were willing to volunteer, plus few other people that were considered knowledgeable on the topic. The questionnaire was delivered also to a branch of national NGOs that deals up with security issues, but unfortunately no one responded, that also speaks loud by itself. Collected information on specific countries is basically received through the use of qualitative methods of research rather than desk research. The findings are based mostly through questionnaires and interviews, and are as presented below.

Albania

This is probably the regional leader when it comes to the institutional set. Albania has established recently a national body that deals with cyber security (ALCIRT – National Security Computer Agency). Unfortunately, the materials are available only in Albanian. Albania also managed to introduce a cyber strategy. This process was supported by the United States Agency for International Development (USAID).[3] One-year program was developed in order to increase governmental capacities on the issues of cyber security.[4] The biggest challenge is implementing and executing the cyber security policies, in reality. The legal framework about cyber security is mostly focused on cybercrime and computer piracy, which is also not enough.

Bosnia and Herzegovina

Bosnia and Herzegovina currently does not have a national body dealing with the issues for cyber security, but all the activities related to the establishment of that body are performed by the Ministry of Security of Bosnia and Herzegovina. This is set by the strategy for establishment of national CERT adopted in 2011. Cyber security issues are affected by different laws such as the law on misdemeanours, law on Protection of Classified Information, law on Protection of Personal Information, law on the Agency for Identification Documents, Registers and Data Exchange, law on Communications in Bosnia and Herzegovina and law on Electronic Signature. A comprehensive approach is again lacking.

Kosovo

There is no national body for cyber security in Kosovo. Kosovo police is responsible for handling cyber security related crimes.[5] The Kosovo Police has taken some initiatives in this aspect in 2011 when they founded a specialized unit responsible for investigating cybercrimes. The unit operates under the directives of the Directorate for Investigation of Organized Crime. This unit consists of law enforcement police officers specializing in crime investigations and experts in the field of information technology. There is no specific strategy dedicated to cyber security, the national security strategy, however, has a section addressing cyber security. When it comes to legal framework, Kosovo has specific law for preventing and combating cyber crimes.

Macedonia

Macedonia does not have official CERT or a national body dealing with cyber security issues. Some preparatory works have been announced through NATO Science for Peace and Security program (Creation of Infrastructure for CERTs in Albania, Macedonia and Bulgaria and their Initial Operation) [6] and representatives of the Directorate for Security of Classified Information and the Ministry of Information Society and Administration, participated in the first meeting of the SEENSA Thematic Work Group (TWG) on Cyber Defence, held on October 23, 2014 in Belgrade.[7] Different stakeholders are engaged in the process such as: Ministry of Interior (MOI), Directorate for Classified Information (DCI), Ministry for Informatics Society and Administration (MOISA), Agency for electronic communications (AEC), Ministry of Defence (MOD), the Intelligence agency (IA), and Directorate for Financial Intelligence (DFFI). There is no officially released cyber security strategy. The only strategy related to cyber issues is the National Strategy for development of Information Society with an action plan (2005). It is expiring, and a new one should be released soon.[8] The legal framework is also diversified. Different aspects are covered by different laws, such as: Law for electronic data and electronic signature, Law for electronic communication, Law for personal data protection, Law on interception of communications, Law on electronic commerce, Law on electronic management (so called e-Government law) and its seven bylaws that facilitate implementation. There is also a national strategy for e-Government for the period 2010-2012.[9] Additional provisions on cyber security issues are affected by the Criminal Code, Law on internal affairs, Law on defence, Law on money laundering prevention and other criminal proceeds and financing terrorism and Law on classified information, as well as the two bylaws for issuing digital certificates in accordance with the law.

The best point about cyber security in Macedonia is the activity of academia in this field. The rising involvement of Macedonian professors and experts in various academic events dedicated to cyber security, development of joint platforms, launching of educational projects and academic curricula in that area are quite promising and with a significant chance of delivering long term results.

Macedonia's Military Academy in the spring 2014 has launched the idea of starting PhD studies and institute for cyber terrorism. If those intentions see realization, Macedonia will get a chance to be the pioneer and a leader in the Western Balkans in this field. Macedonia's military academy has also signed a MoU in cyber defence with the Monterey Institute of International Studies [10] and hosted a number of events dedicated to this issue in the country, such as "Terrorist Use of Cyberspace Advanced Training Course" with NATO's Centre of Excellence on Defence Against Terrorism and the regional training hosted by the Ministry of Defence titled "Dealing with modern security challenges through respect for international humanitarian law: NATO-led operations to counter cyber and hybrid threats."[11]

Montenegro

Research findings on Montenegro have provided a real academic satisfaction in regional context. The country has established a CERT (National CIRT is established at the Ministry for Information Society and Telecommunications) and adopted a national cyber security strategy for the period 2013-2017 that also contains an action plan for strategy implementation (and the document is available also in English). It could be used as a positive example for the other countries in the region. However, there is no specific law on the issue, but it is regulated by a few laws and bylaws, such as the Law on Electronic Trade, Law on information security, Law on electronic signature, etc.

Serbia

Serbia does not have a national cyber security body or a CERT established. Different institutions are dealing with those challenges. Ministry of trade, tourism and telecommunication, Ministry of interior and specialized agencies for security issues like the intelligence agency and the military security agency are in charge. Unfortunately, no one has a clear mandate. Just like in the other countries of the region, there is no specific law adopted; so, there are many legal acts dealing in some manner with this issue like Criminal Code, Law on defence, telecommunications laws, data protection laws, etc. The most specific law on the issue would be the Law on organization and jurisdiction of the state organs in combating high tech criminality. There is the "high-tech crime unit" within the Criminal Police department, and tech-crime prosecutor dealing with cybercrime, but they do have limited capacity and resources. The Ministry of Defence allegedly has a unit protecting its own infrastructure, as does the Ministry of Interior. The academic network is protected by the AMRES project.[12]

The country also lacks a comprehensive cyber strategy. The Law on information security is still in the drafting process. There is a governmental Strategy on the development of information society until 2020 recently adopted, and it provides the framework for development of the so called e-Government.

Why Does Cyber Security Strategy Matter?

The preparation of a cyber security strategy would mean, in the most simplified form considered, allocation of actors, tasks, and responsibilities. Absence of a cyber security strategies in the most of the countries from the Western Balkan is a serious policy gap. The first look at any of the national screenings of the Western Balkan countries that are engaged would provide the reader with confusion and lack of clarity. And for the citizens that live in each of these countries, it is even worse. That is why the drafting of a comprehensive cyber strategy is essential start of the building of cyber security and cyber awareness in the region. Furthermore, cyber security itself is an essential tool for the broader concept of security, quality of life and economic development. It would mean not only increased security, but also increased preparation for Euroatlantic integration of societies. As noted in the OECD 2012 publication "Cyber security policy making at a turning point: Analysing a new generation of national cyber security strategies for the Internet economy," nowadays it is obvious that "the Internet and ICTs are essential for economic and social development and form a vital infrastructure. In a general context of economic downturn, the open Internet and ICTs are a new source of growth and a driver for innovation, social well-being and individual expression. As the Internet economy grows, the whole economy and society, including governments, become increasingly reliant on this digital infrastructure to perform their essential functions."[13] Thereby, the cyber security strategy is the first step on this path.

Regional Cooperation as an Essential Tool

Conclusions can be drawn that all Western Balkan countries are dealing with more or less same challenges and the same situation when it comes to cyber security. The field is underdeveloped or under construction. The reason for such conditions sometimes is the lacking political will, sometimes are capacities missing as well as overall understanding of the problem. Therefore, a broader cooperation with institutions and bodies in the field are necessary. Furthermore, each of them has also some unique solutions that can be shared and compared. On the other hand, good point is when being more or less on the same level, is the fact that it can provide joint contribution and harmonization of the solutions provided at the very beginning, preserving them from later interventions and amending. Additionally, the very nature of cyber domain demands cooperation. Cyber space itself is specific, and it does not recognize borders and nations. Without cooperation, no individual or nation can be truly secure. Third, crucial in this constellation is that cyber is gender, ethnic and nation-neutral. It can affect anyone in the same manner. That is why it can be the perfect topic to be discussed and approached jointly by the Western Balkan states, and serve as a platform for the future, within the safety of provoking bilateral disputes. The Balkans are still far from stable, safe and secure region. Increased vulnerability offline makes space for increased vulnerability online and vice versa. Hence, the finest way is cooperatively to reach some solutions and to overcome the effects of the century long struggles by joint dedication to a field such as cyber security, which is equally important for each of the states, yet as mentioned above, neutral in many ways.

Using cyber security as a platform for cooperation can be a great initial start of many joint regional initiatives and a layer of "second track diplomacy." Of course, a few small countries with limited capacity on the topic probably cannot do much on cyber security; nevertheless, this might be a great incentive for project work with different EU and NATO countries and institutions. In a long term, benefit will be doubled in a manner of regional integration and stability, and cyber security itself.

International Legal and Policy Framework for Cyber Security

The international legal framework on cyber security is pretty vague. Probably this goes in line with the very nature of the cyber space. For such environment, a useful option would be the concept of self-regulation, but it is a mere fact that such approach urges for a very dedicated utilization of the educational and awareness building of the end users.

Secondly, the current legal approach to cyber is pretty narrow, going mostly in line with the criminal law and liability, while what matters for cyber is prevention and deterrence. Also, it is important to underline that cyber security is a broader concept, so a solution framework of the type "one fits all" simply cannot work in such factual environment. The protection of critical infrastructure, data protection, business espionage, energy security and a few more to name are just different sectors in which cyber security does matter. It is crucial to recognize the cyber space as a separate domain, but it is equally important to understand the penetration of the cyber in the different areas that are of vital interest of both everyday life and homeland security.

The most significant documents, internationally speaking, are usually attached to the United Nations. Speaking of which, for cyber security a few resolutions have been adopted by the UN General Assembly:

- Resolution 55/63, January 2001 “Combating the criminal misuse of information technologies”;
- Resolution 56/121, January 2002 “Combating the criminal misuse of information technologies”;
- Resolution 57/239, January 2003 “Creation of a global culture of cybersecurity”;
- Resolution 58/199, January 2004 “Creation of a global culture of cyber security and the protection of critical information infrastructures”; and
- Resolution 64/211, March 2010 “Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures.”

Additionally, various expert groups work in this field. However, those types of documents might be considered as soft law, and represent highly estimated policy response.

Moreover, most prominent in this area is the highly appreciated *Cybercrime Convention* of the Council of Europe.

The Comprehensive study on cybercrime drafted in February 2013 by the United Nations Office on drugs crime noted that “Although no significant developments in the promulgation of a cyber security treaty have been seen in the last decade, the promulgation of international and regional instruments aimed at countering cybercrime have been more successful.”[14] This study refers to the problem through eight different topics:

1. Connectivity and cybercrime;
2. The global picture;
3. Legislation and frameworks;
4. Criminalization;
5. Law enforcement and investigations;
6. Electronic evidence and criminal justice;
7. International cooperation;
8. Prevention.

This approach gives clear picture of the complexity of the problem and the multi-vector approach that should be applied for effective and long terms solutions. The functions of cybercrime legislation in accordance with the same study are settled in the following framework:

- Setting clear standards of behaviour for the use of computer devices;
- Deterring perpetrators and protecting citizens;
- Enabling law enforcement investigations while protecting individual privacy;
- Providing fair and effective criminal justice procedures;
- Requiring minimum protection standards in areas such as data handling and retention;
- Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence.

These goals are complex, since they can easily penetrate into both individual freedom and national security. That is why criminalization looks like the obvious solution. Unfortunately, the costs to deals with the damage done by cyber perpetrators afterwards is often a lot higher than the costs of prevention Cyber security has emerged as a primary concern for many corporate leaders.

A 2014 survey of nearly 500 company directors and general counsel found that “data security” was in fact the number one issue for directors that “keeps them up at night,” and the second most important issue for general counsel is regulatory compliance.[15] Therefore, prevention is the key. And when prevention is the key, usually it starts with human factor and education. Nothing is a guarantee due to the specific nature and context of the cyber security. For this reason, a cornerstone part of the solution might be the self-regulation, activity that requires systematic educational and awareness raising programs for the end users.

Additionally, often there are discussions about the approach – shall it be centralized and specified, such as the dedication and development of cyber security law, or an integrated approach that would mean that cyber security should be the “backup” of every activity.

In the author’s view, the solution is always “*in medias res*” or to be more tangible, somewhere in the middle. It is essential to combine both approaches in order to find effective solutions that fit well with the democratic values as corner stones of modern society. A certain legal framework has to be developed as a basis for further policy modulation. However, speaking from the viewpoint of a lawyer, a closer cooperation between lawyers and engineers, security officers, regulators, academics and practitioners has to develop. Cyber itself acts as a multi vector dimension affecting different stakeholders for different activities. Therefore, finding the appropriate solution would be like solving a puzzle – you need all the pieces together to get the whole picture.

According to the ITU National Cyber Security Guide, the top 10 key cyber security elements to a holistic strategy would include:[16]

1. top government cyber security accountability;
2. national cyber security coordinator;
3. national cyber security focal point;
4. legal measures;
5. national cybersecurity framework;
6. computer incident response team (CIRT);
7. cybersecurity awareness and education;
8. public-private sector cyber security partnership;
9. cyber security skills and training programme;
10. international cooperation.

Meanwhile, we have to keep in mind that data matters, as well as establishing of a CIRT unit and constant improvement is another fundamental feature of a secure cyber future.

Improvements to an incident response team's toolsets and procedures can have a big impact on the Mean Time To Know (MTTK). It is therefore beneficial to measure MTTK so that you can determine the impact of these improvements. Efficiency improvements will also impact the overall mean time to fix, if the organization is tracking that metric from the moment that the incident is identified.[17]

Last but not least, for the Western Balkan countries cyber security is a perfect platform of cooperation. All of the Western Balkan countries have undertaken some initiatives and activities in the field, so it would be both effective and efficient to exchange regionally the local experience. Nonetheless, the region is geographically small, however socially hyper connected and vulnerable. Although the international legal and policy framework is pretty vague, it is enough for a dedicated kick-off. The main problem would be, however, and as always in the Balkans, the political will for action towards something that is in the same time a common problem and a challenge, being free from the burden of history and hate, and of huge interest to the new generations and the youth to work together.

A Possible Way Out

First and foremost, homework for the Western Balkan countries is the preparation and adoption of national cyber security strategies as a way of transposing political will and capabilities into action. However, this process has to be inclusive and transparent. The multi-stakeholder approach is always essential when it comes to security, and this in fact goes for cyber security. Most of the cyber infrastructure is owned by private companies. However, the data protection and the human rights in the cyber sphere are predominantly allocated with the civil society. Each cyber strategy has to be realistic, fact-based and with measurable effects. It is always better to start up with small feasible goals rather than big dreams that are hard to be fulfilled. In the same time, it has to be a governmental initiative due to the fact that, at the very end of the day, even the best strategy falls under the water if political will is lacking. Intergovernmental national bodies to conduct the preparatory work might be one possible solution.

The second step should be to establish national CERT units in accordance with previously adopted strategies.

Furthermore, a process that should go in parallel is the regional cooperation, exchange of know-how and expertise and legal harmonization. For example, harmonization is necessary for the criminal codes as well as for cooperation in prosecuting cyber-related crimes that is on-going through wider regional organizations.

Holding an intergovernmental regional conference will be a good start, and resources could be allocated through different pre-accession or capacity building funds, or through international donors and organizations that currently work on related issues.

Last but not the least, academia and think-tank networking and engaging is essential. The only way for a long term understanding of the problem is in fact education and raising awareness.

Notes:

[1] National Initiative for Cybersecurity Careers and Studies, *Cyber Glossary*, https://niccs.us-cert.gov/glossary, 2014.

[2] European Commission, “Europe’s Future Security Challenges,” 2014, http://europa.eu/rapid/press-release_IP-14-693_en.htm

[3] James A. Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, (Washington, D.C., Center for Strategic and International Studies, 2011), http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

[4] Stephanie Pepi, “USAID Launches the Albanian Cyber-Security Program,” *USAID*, June 13, 2011, https://2012-2017.usaid.gov/news-information/press-releases/usaid-launches-albanian-cyber-security-program.

[5] Kosovo police web site, http://www.kosovopolice.com/, accessed December 2015.

[6] NATO SPS website release, http://www.nato.int/science/studies_and_projects/nato_funded/nigs/nig_982716/nig_982716.htm, accessed 2016.

[7] "First SEENSA Thematic Work Group (TWG) Meeting on Cyber Defence," Announcement at the website of the Directorate for Security of Classified Information of the Republic of Macedonia, Belgrade, October 23, 2014, http://www.dbki.gov.mk/?q=node/400.

[8] Government of the Republic of Macedonia, "Strategy and action plan on informatics society," 2005, www.mio.gov.mk/files/pdf/dokumenti/Strategija_i_Akcionen_Plan.pdf.

[9] Government of the Republic of Macedonia, "Strategy for e-government," 2010, http://www.mio.gov.mk/files/pdf/dokumenti/Strategija_za_e-Vlada-05.03.2010.pdf.

[10] Online news portal announcement, http://www.mkd.mk/makedonija/politika/makedonija-vleguva-vo-sojuz-so-sad-vo-bitka-protiv-sajber-terorizmot (in Macedonian language), accessed December 2015.

[11] Online news portal announcement, http://213.133.111.76/makedonija/vesti/159497-Regionalna-obuka-od-oblasta-na-megunarodnoto-humanitarno-pravo (in Macedonian language), accessed December 2015.

[12] Belgrade University Computer Centre, "Web announcement," http://www.rcub.bg.ac.rs/en/projekti/arhiva-projekata/108-academic-network-of-serbia.html, accessed December 2015.

[13] *Cybersecurity Policy Making at a Turning Point, Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (Paris: OECD, 2012) www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[14] United Nations Office of drugs and crimes, *The Comprehensive study on cybercrime; 2013*, 2013, https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[15] Allison Grande, "Data Breaches Put Retail GCs in the Firing Line," *Law360*, New York, May 21, 2014, http://www.law360.com/articles/537810/data-breaches-put-retail-gcs-in-the-firing-line.

[16] Frederick Wamala, *The ITU National Cyber Security Guide* (Geneva: International Telecommunication Union, September 2011).

[17] Ponemon Institute, *Cyber Security Incident Response: Are We as Prepared as We Think?*, 2014.

About the Author

Vesna POPOSKA holds a master degree in International law and international relations from the Faculty of Law "Iustinanus Primus" in Skopje. Currently she is a PhD studies in International relations and security at the Military Academy "General Mihailo Apostolski" in Skopje. She is actively engaged in Macedonian higher education and research area as a teaching assistant and trainer in international law. Currently, she works for the International Vision University as a Secretary General, as well as alumni of the School of Politics of the Council of Europe, alumni of President Ivanov School for Young leaders, and Jean Pictet moot court competition. She has participated in training and conferences in the country and abroad as speaker and contributor and has published several papers on legal frameworks for cyber security, counterterrorist operation, international human rights law, and international humanitarian law.