ARMENIAN NATIONAL POLICY IN CYBER SPACE

Toward a global cyber security architecture

Ruben Elamiryan

Introduction

This chapter presents the cyber security of Armenia by considering its national security system, as well as integration into regional and global cyber security architectures. It demonstrates that currently Armenia is a less developed actor globally, however it is a factor of stability in the regional cyber security architecture. Nowadays Armenia is in the process of the establishment of a more comprehensive and sophisticated cyber security system to provide more active participation in the global cyber security. The major challenges which Armenia faces in cyber space are presented through three-level analysis: national, regional, and global. However, the more vital threats come from Azerbaijan and Turkey with regard to the Nagorno–Karabakh conflict and recognition of the Armenian Genocide of 1915.

At the same time, Armenia faces a transformation of the cyber security approaches caused by the rising challenges and threats in global and regional cyber space. Many of the concepts and norms in the field of cyber security expressed in Armenian documents in 2009 appeared to be influenced by Russian understandings (for instance, the use of term “information security,” which integrates both information-psychological and information-technical components of cyber security); the draft version of the Cyber Security Strategy (HH kiberanvtangutyan nakhagits, 2017) provides more Western approaches to cyber security. However, having strategic relations with both the West and Russia, Armenia tries to integrate the best practices from all sides.

The above becomes clearer from the research of Armenia tightly cooperating, particularly in cyber security, with the North Atlantic Treaty Organization (NATO) while being a member of the Russia-led Collective Security Treaty Organization (CSTO) (NATO, 2016). The relations with other international organizations, such as the United Nations (UN), Organisation for Security and Co-operation in Europe (OSCE), International Atomic Energy Agency (IAEA), and Shanghai Cooperation Organization (SCO) witness rather “on hold” relations, at least publicly.

The concept of cyber security

The terms “cyber security” and “cyber defense” are multifaceted, leading to differing interpretations of each. Some perceptions concentrate solely on the military dimension of the issue, while others include a systems approach with both civil and military dimensions.
Based on the above, I will suggest the following definition of cyber security which will be the working one for this chapter:

Cyber security is a set of technical and non-technical (policies, security arrangements, actions, guidelines, risk management) measures which provide for the social, ethnic and cultural evolutionary modernization of the critical cyber infrastructure, as well as protection of vital interests of human, society and state.

(Elamiryan & Bolgov, 2018)

At the same time, a sophisticated cyber security system supposes forecasting and preventing cyber threats at early stages, as well as not only the ability to face challenges but also raise them when necessary.

**Cyber security in the Republic of Armenia**


With regard to the cyber component of these documents, none of the above-mentioned strategic documents contains information strictly on cyber components. They do not bring clarity to the notion of critical cyber infrastructure, either. At the same time, for instance, the military doctrine of Armenia sets official views with regard to, specifically, the military-technical dimension of military security of the RA. Moreover, the technical and infrastructural components, as well as the information systems, are viewed separately as components of military security.

The research of the National Security Strategy of the Republic of Armenia concludes that cyber security is considered an instrument for effective functioning of information-psychological components of information warfare. For instance, it states: “Therefore, the Republic of Armenia aspires to … integrate into the international information area, to ensure professional promotion of Armenia and the Armenians, and to counter disinformation and propaganda” (National Security Strategy of the Republic of Armenia, 2007).

In this context, the Concept of Information Security (it is outdated, but we do not have a new one published yet) brings more clarity in the cyber field of Armenia. As in Russia and some other post-Soviet countries, it views cyber security in the broader context of information security, particularly, as the information-technical component under the umbrella term of information security. That is the reason why the Concept discusses cyber issues twice, but only in the context of cyber-crime issues.

However, the deeper comparison of the Armenian and Russian cyber security systems (Elamiryan & Bolgov, 2018) allows us to determine that, despite the tight military cooperation, the two countries do not share equivalent cyber security approaches. For instance, both countries do not have a centralized cyber command, however, Smirnov and Zhitnyuk believe that in Russia the technical aspects of cyber security are under the monopoly of the Federal Security Service (FSB in Russian), since all structures are obliged to use means of information protection, certified by the FSB (Smirnov & Zhitnyuk, 2010). In Armenia the provision of cyber security is rather de-centralized. Unlike Russia’s troops of information operations, which were established in Russia in 2014 and whose functions
include all aspects of information warfare: from psychological operations and propaganda (including the Internet) to the security of computer networks and cyberattacks on the enemy’s information systems (Elamiryan & Bolgov, 2018), Armenia’s cyber troops focus exclusively on the information-technological domain.

At the same time, while Russian analysts and policymakers tend to emphasize cyber sovereignty stating that “the main idea is that the government (in Russia) should have means of control over cyberspace and information traffic in order to ensure digital sovereignty but not to fence off the global network” (Elamiryan & Bolgov, 2018: 7), Armenian policymakers are more likely to provide rather liberal cyber space in Armenia, not really sharing Russia’s understanding of cyber and digital sovereignty. The principle is “allow everything that is not prohibited,” when prohibited are direct and clear criminal acts. For instance, the history of Internet in Armenia could hardly remember a single case when government blocked social media during anti-government demonstrations (Elamiryan & Bolgov, 2018).

It is also worth mentioning that the Russian analysts think that “the Russian approach focuses more on the security of information itself leaving the infrastructural level as a complementary component,” when cyber space is considered to be a narrower notion as “a well-defined element of the information space” (Elamiryan & Bolgov, 2018: 1–2).

This demonstrates that nowadays (at least before the Armenian Velvet Revolution) Armenia is transforming its post-Soviet (Russian) view of information/cyber security to separation of the information-psychological and information-technological components of the general information security system. This is partially evident from the transformation of the names of documents: Information Security Concept (the Concept) in 2009 and Cyber Security Strategy (the Strategy) (HH kiberanvtangutyan nakhagits, 2017) in 2017–2018. Although the latter is not publicly available, its draft is available at the web site of the Ministry of Transport, Communication, and Information Technologies of the Republic of Armenia. The draft is a long-term cyber security development plan for Armenia and provides the relevant timeline for its implementation. It supports the above assumption on transformation of cyber security approaches from post-Soviet reality to more Western perceptions. Particularly, along with the clear-cut separation of the cyber security from information-psychological realm, the Strategy outlines a comprehensive development agenda, including establishment of a cyber security centre to coordinate the cyber security activities in Armenia (HH kiberanvtangutyan nakhagits, 2017). However, the implementation of this agenda is the matter of the upcoming future.

At the same time, despite the availability of a number of normative acts for cyber space in Armenia, it is hard to claim that they derive from the Concept. Rather, the transformation of cyber space in general, as well as the arising global, regional, and local threats and challenges provokes development of new regulations, for instance, the Law of the Republic of Armenia on Protection of Personal Data, which regulates the procedure and conditions for processing personal data, exercising state control over them by state administration or local self-government bodies, state or community institutions or organisations, legal or natural persons (Law of the Republic of Armenia, 2015).

Continuing the discussion about the normative part of cyber security in Armenia, an Armenian expert in cyber security, Samvel Martirosyan, put it the following way: “The normative part is rather underdeveloped, as most of the legal norms are rather old (except a recent law on personal data protection accepted in 2015).” He continues and explains that the Concept of 2009 was adopted based on the post-soviet experience of information security. In particular, it does not separate cyber security from propaganda/antipropaganda.
As a consequence, on one hand, it discusses the issue as a system, but on the other hand it brings uncertainty in the field. “Now we have the problem of clarification for ourselves the concepts of cyber security, cyber space, as well as critical cyber infrastructure.” According to Martirosyan this situation causes very liberal cyber space in Armenia without filtering or blocking any cyber subject (except two short cases in 2008 and 2016). At the same time he mentions that the new cyber security strategy (accepted in 2017, but not yet publicly presented) “will allow us to develop the field more rapidly. And I think we will see it in the new concept of information security of Armenia.”

Another Armenian expert, the CEO of the private cyber security company CYBER GATES, Samvel Gevorgyan, during the expert interview with me made for this chapter, clarified that the level of cyber security in Armenia is rather low, but it is experiencing a gradual rise. According to him, some parts of Armenian cyber space are protected by the National Security System of Armenia which led to the gradual decrease of successful cyber operations against the Armenian cyber space. At the same time the Ministry of Defence of Armenia, the Police, and the National Bureau at the National Academy of Sciences, as well as some private companies, work to provide security for specific fields in the cyber domain. “However the problem is that there is a low level of coordination among them,” concluded Gevorgyan.

Rather problematically, the issue of the leading role in carrying out cyber security activities, as well as clear separation of responsibilities, are not addressed by the Concept or any other strategic document. This does not clarify if any ministry or organization is given this role, however it is not available publicly.

In this context Gevorgyan stresses the importance of public–private cooperation to provide cyber security for Armenia:

Currently we face gradual rise of public–private cooperation in cyber security. For instance, as a private company we cooperate with the Police, National Security Service, and judicial system. Very often we start from one-time activity, which later transforms into long-term collaboration.

As a good example of private–public cooperation Gevorgyan mentions the functioning of the www.april2016.am website, which was established by private donors with the support of the Ministry of Defense of Armenia. The cyber protection of the website is provided by the private CYBER GATES. The website was established after the so called “April war” – a massive military escalation, initiated by Azerbaijan against the de-facto Nagorno-Karabakh Republic. As the website provides comprehensive information and the Armenian view of the “April war,” it faces regular massive cyberattacks from Azerbaijan. “It is the number-one target, but the Azerbaijani hackers cannot eliminate it,” states Gevorgyan. In addition, it is worth mentioning that this cooperation does not have strategic and/or normative basis and regulation, and is in the process of transforming its ad hoc nature into long-term reality.

Thus, we can see that the normative component of cyber security in Armenia currently experiences the process of strategic formation. As many other countries which recently came across the cyber issues, full scale cyber or hybrid warfare, Armenia first of all should clarify the general vision of its cyber security system. This will allow it to provide strategic and operational normative frameworks as the first step to formulate and implement practical policy-making in cyber domain.

In the meantime, this process should take place as soon as possible, because the cyber field is one of the most rapidly developing in the world and it will not wait for the actors of
international relations to catch up with them. In this context the next section of this chapter
draws out the main challenges and threats to the cyber security of Armenia which the
country faces or could face in the near future.

**Key challenges and threats to Armenian cyber security**

The examination of the above presented strategic documents, as well as the necessity to
provide multilayer security for critical cyber infrastructure of Armenia allows drawing out
the most perilous symmetric and asymmetric threats and challenges to cyber security of
Armenia. They could be grouped into the three-level system that follows.

**The national level**

This level includes threats to critical cyber infrastructure, lack of high-quality cyber security
specialists, brain-drain, and limited digital literacy of the population, as well as too free
internet space, and a low level of normative regulations. Particular threats come from social
media and social networks. Another serious threat is the limited level of democratic
development. In this regard Armenian scientist, Mamikon Margaryan (2013), believes that
establishing the principles of “good governance,” run by strategic leaders, can become an
effective measure to modernize the cyber security system in the region of the South
Caucasus, not only on an information-technology level, but also to increase the
responsibility of political leaders and maximize improvement of cyber security in the RA.

In this context, Gevorgyan mentions the challenge of public awareness and Armenian
mindset. According to him, on one hand the victims of cyberattacks in Armenia try to keep
it secret when they are attacked and hacked. On the other hand, people and businesses do
not want to pay for cyber security. As a result, these two factors together make the field
more vulnerable. “It is very important to change this approach and as a private company we
are working in this direction,” states Gevorgyan. Interestingly, Gevorgyan finds the private
sector in Armenia more secure then the public one. He explains: “Despite the private sector
experiencing more deliberate attacks, but most of the private companies have their own
rather professional cyber security teams (for instance banks). The public sector is protected
only partially by, for instance, National Security Service.”

**The regional level**

Being part of the South Caucasus and the Near East, Armenia faces a wide range of regional
threats, particularly in cyber space. These issues deeply affect human security, which is
a comprehensive set of threats directed against personal cyber security, as well as to control
human feelings, emotions, psychological conditions, and the ability to objectively perceive
physical and virtual realities (Elamiryan, 2015). A large volume of information appears daily in
conventional and social media and is aimed at influencing human perceptions in different
countries. The countries of both the South Caucasus and the Near East region strive to foster
political stability and sustainable development. However, in our view, neither success nor
failure in cyber operations can provide long-lasting sustainable development. At the same time
the most vital threats to Armenian cyber security on a regional level come from its two
neighbors Azerbaijan and Turkey. The reason is the ongoing Nagorno-Karabakh conflict
between Azerbaijan and self-determined unrecognized Nagorno-Karabakh Republic. In this
conflict Armenia (whom Azerbaijan claims to be the main side of the conflict) supports the
Armenian populated Nagorno-Karabakh Republic, while Turkey supports Azerbaijan. As a result, we now witness full-scale cyber warfare, to say the least, between Azerbaijan and Turkey, on one side, and Nagorno-Karabakh Republic and Armenia, on the other (Kotanjian, 2009; Elamiryan, 2015; Martirosyan, 2017).

There is no specific data on the quantity and quality of cyberattacks initiated by the two sides. However, frequently various local news agencies share information regarding successful or unsuccessful attacks on public and private resources committed by both sides (Jnews, 2011; Armenpress, 2012; The Register, 2016; Telecom Arka, 2018).

It is worth mentioning that full-scale cyber warfare accompanied the “April war.” During the four days of war all the sides – Azerbaijan, Nagorno-Karabakh Republic, and Armenia – initiated and faced the whole spectrum of cyber operations, including DDoS attacks against news outlets and public institutions, operations in social medias (Facebook, Twitter), and so on (Tovmasyan, 2016).

Interestingly, in this context Gevorgyan thinks that Armenia gains much experience from Azerbaijani cyber operations. According to him, rather often these operations are successful, but they sophisticate the Armenian forces.

The global level

Globalization and development of networked society raises the issues of global cyber security due to the following:

- Vulnerability of the global cyber infrastructure, as a consequence of all the many actors involved in this process.
- The threat of communication manipulation.
- Underrepresentation in global cyber space.
- Crisis of multiculturalism.
- Dichotomy of traditional and modern values.
- Threats to sovereignty.
- Atomization of society, when a person only formally feels itself as a member of that society/state based on its current needs.
- International crime and terrorism, which are largely presented in cyber space.

Talking about regional and global threats towards the cyber security of Armenia, Martirosyan outlines the following:

- One of the main threats is Azerbaijan, which works against Armenia also in cyber domain. It takes place not only on state level, but also on behalf of formal-patriotic entities. “For instance the largest hacker group in Azerbaijan is called Anti-Armenia,” Martirosyan clarifies.
- Another big issue for Armenia is the so-called state-sponsored attacks, which are directed deliberately against public figures and journalists in Armenia to receive information and frame public opinion. These attacks have different interested countries as subjects, not only Turkey and Azerbaijan.
- One more challenge is the attacks against the banking system, which gradually becomes a target. This is a relatively new challenge and banks have to work hard to be able to face the rising threats.
This section clearly demonstrates that nowadays Armenia faces a wide range of cyber challenges and threats, even cyber warfare, on national, regional, and global levels. At the same time, not a single small- or medium-size country is able to unilaterally provide effective solutions to the rising issue, let alone the development of early-prevention mechanisms. From this perspective Armenia does its best to integrate into regional and global security systems to provide more comprehensive and effective cyber security nationally, regionally, and globally.

**Armenia within the context of regional and global cyber security architecture**

Nowadays most of the international organizations (global and regional) have expanded their security agendas to reflect on rising challenges and threats of cyber security. The UN, OSCE, Shanghai Cooperation Organization (SCO), International Atomic Energy Agency (IAEA), NATO, Collective Security Treaty Organization (CSTO), and so on are developing strategies and operational capabilities to provide a more manageable and secure cyber environment.

Armenia, as an active member in the international community, is largely involved in the formation of global and regional cyber security architecture. In this regard Martirosyan thinks that Armenia is rather active in terms of international cooperation. However, the issue here is that the country has to work with and between both West and East, which very often have rather different approaches.

On the other hand, currently it is difficult to see any effective cyber security developments with the UN, IAEA, or OSCE, of which Armenia is a member. Moreover, the Memorandum on granting the Republic of Armenia the status of SCO dialogue partner was signed on April 16, 2016 at the SCO headquarters in Beijing. However, there is no publicly available information on the cooperation of Armenia with these organizations on cyber security issues. Due to the certain level of secrecy, the experts from government who are in charge of cyber security and work with these organizations also remain silent.

At the same time the following extract from the special address of the OSCE Secretary General Thomas Greminger on “The Future of European Security: Managing East-West Relations,” chaired by Professor Wolfgang Danspeckgruber at the Liechtenstein Institute on Self-Determination at Princeton University on September 28, 2018, (with some reservations) could describe the situation with cyber security in institutions of collective security:

Now in terms of thematic expertise, when it comes to relatively new security challenges, we still need to build our expertise on these issues. And this depends automatically on the will of participating states to give us the necessary resources. And here we clearly face challenge – we have [an] understanding of the relevance of these issues, and on the other side – strict budget policies, which makes it very difficult to develop this kind of issues. I am not going to tell you how many staff I have on cyber security, because you simply will not believe me. But this is a challenge. When it comes to more conventional security issues, we have fantastic capacity and institutions, but with new security issues, we face challenges to bring the necessary expertise into our discussions.

*(Greminger, 2018)*
Based on the above, we should admit that at this point collective security organizations are less effective than collective defense ones. For this reason, this part will stop only on Armenia-NATO cooperation and Armenia’s CSTO membership, where the results of collaboration are more or less tangible.

**Armenia-NATO cooperation: cyber security dimension**


Key areas of cooperation include: security cooperation, defense and security sector reforms, civil emergency planning, science and environment, and public information. Currently, Armenia is implementing its fourth Individual Partnership Action Plan for 2014–2016, which was approved on May 23, 2014. At the same time, Armenia is an active contributor to NATO-led operations in Afghanistan and Kosovo. In 2007, a NATO information center officially opened in Yerevan (Relations with Armenia, 2016).

In this context, it is necessary to analyze the current state of Armenia-NATO relations in the cyber field, including the perspectives of each player regarding cyber security, as well as opportunities for further development in the cyber security field.

The 2014–2016 IPAP for Armenia lists five main actions to enhance Armenian capabilities for protecting critical communication and information systems against cyberattacks. They include conducting a study of international best practices in cyber security; establishing a network monitoring system in the National Security Strategy of Armenia; establishing response procedures for identified threats, providing methodologies, professional manuals, and other relevant materials to Armenia’s cyber security state agencies, relevant departments, and professional training organizations; and harmonizing Armenia’s national legislation with international legal norms addressing cyber space (IPAP, 2014).

A comparison of 2009 IPAP and 2014–2016 IPAP demonstrates the positive evolution of Armenia-NATO cyber cooperation in developing new approaches and addressing new elements of cyber security. However, interviews of experts lead to the conclusion that, in reality, Armenia-NATO cooperation in cyber security is limited to participation of the representatives of the Ministry of Defense and Armed Forces of the RA in NATO-organized seminars, conferences, and training. This development is partially reflected in Global Cybersecurity Index, as shown in Table 3.1.

<table>
<thead>
<tr>
<th>Year</th>
<th>Country Index</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>0.495</td>
<td>79</td>
</tr>
<tr>
<td>2017</td>
<td>0.196</td>
<td>111</td>
</tr>
<tr>
<td>2015</td>
<td>0.176</td>
<td>23</td>
</tr>
<tr>
<td>2014</td>
<td>0.176</td>
<td>23</td>
</tr>
</tbody>
</table>

There was no change during 2014–2015. Interestingly there was a similar tendency of “stability” in the whole region of the South Caucasus for 2014 and 2015.

However, the International Telecommunication Union (ITU), which calculates Global Cybersecurity Index has changed the methodology for 2017. As a result, it completely changed the picture, as shown in Tables 3.2 and 3.3:

Commenting on the low position of Armenia in Global CyberSecurity Index, Martirosyan and Gevorgyan agreed the calculation of the Index is rather technical and in practice Armenian cyber security capabilities are rather strong. “For instance, Georgia’s position is high in the ranking as it is much more open to work with international agencies and follow their formal normative requirements, what we cannot say about Armenia”, Martirosyan explains. This explanation could be true, as during this research I tried to implement expert interviews with government officials in cyber security, however I failed due to the certain restrictions and secrecy in work of the relevant agencies and their employees.

Continuing with the analysis of cyber security cooperation between the RA and NATO based on DOTMLPF II components – Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Interoperability, and Information – there is a clear demonstration of rather well-developed cooperation in normative and education, but with greater potential for development in other fields.

From this perspective, DOTMLPF II could become the framework to modernize Armenia-NATO relations in cyber security (see Table 3.4).

Furthermore, Armenia-NATO cyber security cooperation must go beyond a purely technical and technological framework. Nowadays mankind, and specifically the nations of the South Caucasus, faces regional and global challenges and threats which undermine national, regional, and global stability. Consequently, humanization of cyber space and
development of a culture of cooperation in the South Caucasus will support sustainable development not only for that region, but also for wider areas of Eurasia and beyond. In this context, NATO can be one of the key actors in the humanization of cyber space, based on promoting a culture of peace and cooperation in the South Caucasus through, for instance, cyber security training, which NATO conducts for the countries of the South Caucasus.

The Collective Security Treaty Organization (CSTO)

Armenia became part of the then-Collective Security Treaty back in 1992 and from 2002 joined the then-newly formed CSTO (on the basis of Collective Security Treaty) as a full member.

The CSTO Charter’s key Article 4 states that if one of the Member States undergoes aggression (armed attack menacing to safety, stability, territorial integrity and sovereignty), it will be considered by the Member States as aggression to all the Member States of this Treaty. Accordingly, all the other Member States at request of this Member State shall immediately provide the latter with the necessary help, including military assistance (Collective Security Treaty Organisation, 1992).

However, a question can be raised if this Article covers the issues of cyber security, too. Further clarification, particularly with regard to information field, is provided by Article 8 of the Charter, which states that, “… Member-states interact in fields of border protection, information exchange, information security, protection of population and territory from emergency situation of natural and technogenic character, as well as from dangers derived from military actions” (CSTO Charter, 2002).

More details in this regard are provided both in the “On the Strategy of CSTO collective security for the period till 2025”, approved by the decision of the CSTO Council.

Table 3.4 DOTMLPF II and Armenia-NATO Cooperation

<table>
<thead>
<tr>
<th>DOTMLPF II Component</th>
<th>Possible Modernization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctrine</td>
<td>The IPAP for 2014–2016 covers the standard elements of Armenia-NATO relations. However, a separate joint strategy is needed and should be devoted specifically to cooperation in cyber security.</td>
</tr>
<tr>
<td>Organization</td>
<td>The actors can establish a joint center for coordination of cyber security in areas of mutual interest.</td>
</tr>
<tr>
<td>Training</td>
<td>Training in cyber security should be expanded for the Ministry of Defense and Armed Forces of the RA, and should include other ministries and civil institutions as deemed necessary.</td>
</tr>
<tr>
<td>Materiel and Logistics</td>
<td>A joint cyber infrastructure should be developed to predict and to eliminate threats in their early stages.</td>
</tr>
<tr>
<td>Leadership</td>
<td>Tighter cooperation and communication should be developed between the leaders of Armenia and NATO that are responsible for cyber security.</td>
</tr>
<tr>
<td>Information</td>
<td>Pertaining to the establishment of the joint center for cyber security coordination, a mechanism of information exchange on cyber issues of mutual interest should be developed.</td>
</tr>
</tbody>
</table>

Source: IPAP (2014).
on October 14, 2016 (the Strategy 2025) and the Agreement on cooperation in provision of information security, accepted by the majority of the CSTO member states during the session of the CSTO Council on November 30, 2017. Particularly, the Strategy states that “one of the main modern threats and challenges to CSTO collective security is the aspiration to achieve strategic goals by use force, including information oppression, use of information-communication technologies to provide destructive impact on social-political and social-economic situation, manipulation of public consciousness in so called ‘complex’ or ‘hybrid’ technologies” (Strategy, 2016).

Generally speaking, the CTSO pays increasing attention to the provision of information security. However, neither the Charter nor various high-level declarations provide clue on whether Article 4 of the Charter also refers to information aggression, and how the CSTO member states would coordinate and combine their efforts to withstand information operations against any of them.

At the same time the Agreement (Republic of Kazakhstan, 2016) describes the CSTO perception of “threat to information security” as factors (integrity of factors), which create danger for people, society, and state in the information field. The document separates threats into three groups:

- Destructive impact on CSTO member states and the CTSO in general.
- Use of information-communication technologies by terrorist and extremist organizations and organized crime.
- Criminal acts with use of information-communication technologies.

What is interesting is that CSTO experts see cyber security (or the information-technological component of information security) as an integral component of broader information security. As a consequence, most of the CSTO strategic documents use the umbrella term “information security.” The latter encompasses both information-technological (including cyber domain) and information-psychological components of the security architecture. We also see this approach in Armenia. At the same time neither the Strategy (2016), nor Agreement (Republic of Kazakhstan, 2016) and Charter (2002) use the term “cyber security” and “cyber warfare,” in particular, in contrast to the NATO approach. Hypothetically, the terms differ from each other depending on the foreign policy of the country.

The Strategy (2016) emphasizes the formation of secure information space of CSTO member states as the main CSTO information security strategic goal, which undoubtedly also includes cyber domain. At the same time, according to the Strategy (2016), the CSTO should undertake the following set of actions to guarantee comprehensive information security for the member-states:

- Formation of CSTO member-states’ information security system;
- Development of interstate and inter-institutional cooperation in information security;
- Modernization of mechanisms to counteract threats in information space;
- Implementation of joint events to counteract and neutralize threats in CSTO information-communication space;
- Interaction in international information security provision issues;
- Development of coordinated rules of behavior in information space and its promotion to international level;
- Development of conditions to establish basis for coordinated information policy.
Based on the Strategy (2016), the Agreement (Republic of Kazakhstan, 2016) presents more details and practical solutions to provide CSTO information security agenda on the ground. Article 4 of the Agreement defines the following directions of cooperation:

- Development of joint legal bases;
- Formation of practical mechanisms for joint reaction to threats to information security;
- Trust enforcement measures;
- Modernization of technological basis of information security;
- Establishment of the necessary conditions for the development of inter-institutional cooperation of the member states.

Articles 5 to 8 of the Agreement provide detailed clarifications and practical mechanisms on each above presented direction, which encompass a wide range of measures to coordinate and jointly secure CSTO information space from both information-psychological and cyber (not naming it) perspectives.

In this regard it is notable that back in 2014 information appeared that the CSTO member states were planning to establish a joint center for reaction to cyber incidents (CSTO will launch …, 2014). However, we do not see any progress with regard to this suggestion either in Strategy 2025, or in the Agreement.

As effective implementation of any strategy demands well-organized structure, it is necessary to understand the relevant institutional framework, which is responsible for the functioning of the CSTO and, specifically, of its information security wing.

The CSTO organizational structure clearly demonstrates that there is only one division, which is directly responsible for the provision of information security (CSTO Structure, 2017). At the same time Bondurovskiy (2016) stresses the importance of the CSTO Parliamentary Assembly in information security as it coordinates the activities on harmonization of national legislatures.

Another two important organizations, which promote the CSTO information security, but are not direct divisions of the organization, are the Analytical Association of the CSTO and the CSTO University League. These two organizations provide academic partnership and university cooperation among the member states, organizing various academic-practical events (CSTO University League, 2014).

At the same time, one of the most successful proofs of the CSTO joint activities in information security could be the so-called PROKSI operations (from Russian, Counteraction to Crime in the Sphere of Information). The main goal of the operation is to reveal and suppress the functioning of such information resources in national segments of internet, the content of which damage or can damage national and collective security of the member states. PROKSI started in 2009. Since that time about 80,000 dangerous information resources were revealed (From Treaty to Organization, 2017).

Thus, we see that nowadays, in terms of information and cyber security on an institutional level, the Organization is in the process of development and operates mostly within the framework of the coordination of efforts. However, the problem is that the CSTO member states very often have, if not conflictual, at least different interests not only in terms of information security, but also with regard to the Organization’s general activities. The latter largely impedes the effective functioning of the strategic goals for all member states, including Armenia.
Conclusion: the future of cyber security in Armenia

This chapter clearly demonstrates that nowadays Armenia is in the process of the development of a comprehensive and sophisticated cyber security system. In this process, Armenia conceptualizes cyber security as a combination of individual and collective good, which, as a consequence, should be pursued both unilaterally and through the development of regional and international regimes.

In this regard it is developing normative frames (cyber security strategy, laws, and so on), domestic institutions, and operational capabilities. On the other hand, Armenia integrates and develops in cooperation with regional and global international organizations. Particularly, we witness rather “on hold” relations (at least publicly) with the UN, OSCE, IAEA, and Shanghai Cooperation Organization and more active collaboration with institutions of collective defense such as NATO and CSTO.

With respect to the necessary developments in cyber security systems in Armenia, Martirosyan, during the expert interview, specified the following:

- Final clarification of the vision, ideology, and philosophy to provide security in cyber space.
- Modernization of the legal bases of cyber space.
- Establishment of an executive body or bodies to be responsible for cyber security.
- Development of public education in cyber security.

“This should be enough for the start, as it is dangerous to implement all the changes at once and all together. This can lead to enormous regulations and groundless restrictions to freedom in cyber space,” stated Martirosyan in an expert interview arranged for the purpose of writing this chapter.

Agreeing with Martirosyan, however, it is necessary to emphasize that the main challenge to cyber space today is its internationally fragmented character. The problem is that the international community in general does not have a clear vision of tomorrow and, as a consequence, how to face the current and future challenges and threats in cyber space. This makes the countries deal with the threats alone – a task that is completely impossible for small and medium-sized entities. The rising regional and global uncertainties are also reflected in the cyber field, making it more essential to accelerate the modification of global and regional security institutions to bring more clarity, cooperation, and peace into the so called fifth geopolitical domain.

Suggested reading


References


Armenian national policy in cyber space

