Stiftung Neue Verantwortung

Exercise Background Material

Armenia
Country Profile

Points of Contact: Rebecca Beigel, Julia Schuetze, Lina Siebenhaar | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us. The country profile was published in April 2022.

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Lina Siebenhaar

Student Assistent for International Cybersecurity Policy

lsiebenhaar@stiftung-nv.de

Table of Contents

Political System and Socio-Political Background

Key Facts

- Official country name: Republic of Armenia[1]
- Capital: Yerevan city[2]
- Population: 2'961'000 (as of January 2022)[3]
- Official language: Armenian[4]
- Currency: Dram[5]

Political System

Armenia is a unitary multiparty republic.[6] The Constitution, adopted through a referendum in 1995, establishes the separation of the legislative, executive, and judicial branches.[7] The President of the Republic is the head of state. Since March 2022, this role has been held by the independent Vahagn Khachaturyan.[8]

Nikol Pashinyan, a member of the Civil Contract Party, was appointed Prime Minister for the second time in 2021.[9] The Prime Minister is tasked with elaborating the government's policy and coordinating and leading its work.[10] The unicameral legislative branch consists of the National Assembly.[11] The highest instances of the judiciary are the Court of Cassation and the Constitutional Court.[12]

Socio-Political Context

Since independence from the Soviet Union, the Armenian economy has undergone profound changes. Until the global financial crisis of 2008, Armenia's economic transformation was considered "an important success story among the transition economies."[13] However, recovery from the crisis has been slow, and poverty and economic growth levels have only slowly returned to pre-crisis levels.[14] The GDP growth rate for the period of 2012-2016, for example, is ten percentage points lower than the rate of the years 2005-2008.[15]

Key challenges to the economy's recovery include out-migration and aging in society, with a 0,2 percent average annual decrease in the population.[16] Another difficulty for Armenia is the outdated and inadequate infrastructure. This is illustrated by the fact that the country's transportation infrastructure ranked 101 out of 167 in a 2012-2018 World Bank report and

116 out of 167 in the Logistics Performance Index, where infrastructure is one of six application criteria.[17] Digitalization plays a crucial role in the development of public sector services and Armenia's economic growth more broadly. This is recognized by the introduction of "Armenia's Digitization Strategy 2021-2025," aiming to transform government, society, and the economy (see section "Key Documents" below).[18]

In addition to the challenges mentioned, the combined crisis of the escalating violent conflict over the Nagorno-Karabakh region[1] with the neighboring country of Azerbaijan and the COVID-19 pandemic hit Armenia in 2020.[19] Both led to a 7,4 percent contraction of the economy and a sharp increase in poverty levels. The lower middle-income-poverty rate rose from 9,8 percent in 2019 to 12,5 percent in 2020.[20]

The situation in the Nagorno-Karabakh region also affected Armenia's freedom online. According to the Freedom on the Net Report 2021, Armenia is considered a free country that mostly respects the rights of internet users and the freedom of speech. However, during the escalating violent conflict in the Nagorno-Karabakh region, various restrictions on Internet freedom were registered, including the blocking of websites and other restrictions legitimized by martial law.[21] This is also why Armenia dropped two ranks in the 2021 World Press Freedom Index compared to the previous year, falling from 61st to 63rd out of 180.[22] According to Reporters without Borders, transparent "media ownership and journalistic independence are still far from being achieved."[23] According to data from 2019, 66,5 percent of all individuals in Armenia had access to the internet.[24] The most important means of access to the internet are smartphones, with 121,3 smartphone subscriptions per 100 people.[25] In its 2019 Global Competitiveness Report, the World Economic Forum ranks Armenia's adoption of Information and Communication Technologies (ICTs) 59th out of 141, with an upward trend.[2]

1 In 2020, the ongoing "violent crisis over contested territories, particularly the Nagorno-Karabakh region, between Armenia and Azerbaijan escalated to a war. The Nagorno-Karabakh region is mostly inhabited by ethnic Armenians and supported by Armenia, but is internationally recognized as a territory of Azerbaijan" (Heidelberger Institute for International Conflict Research (2021): Conflict Barometer 2020). The designation of the violent conflict as the "Nagorno-Karabakh" conflict used in this report is based on the OSCE Minsk Group's work. The OSCE Minsk Group is the only internationally mandated format for conflict settlement (OSCE (n.d.): OSCE Minsk Group.; The President of the Republic of Armenia (n.d.): Artsakh Republic: History and Current Reality.)

2 In its 2019 Global Competitiveness Report, the World Economic Forum ranks Armenia's adoption of ICTs 59th out of 141, with an upward trend.

Armenia's Cybersecurity Policy

Vulnerability and Threat Landscape

In the past, Armenia experienced a number of cyber incidents that targeted different sectors and parts of society and gained public attention.[26] These incidents include the Tainted Leaks, uncovered in 2017. Individuals from the military, government, administration, and civil society were targeted to gather information.[27] Other cases include the operation Red October, where Armenia was among the ten most-affected countries,[28] and an operation by the group APT28 that targeted the Armenian military by mimicking the domains of existing organizations.[29]

A large proportion of small- and medium-scale cyber operations appear to be motivated by political objectives in the context of the escalating violent conflict in the Nagorno-Karabakh region (see section "Socio-Political Context").[30] In January 2016, for example, various Armenian government websites and websites of Armenian embassies in more than 40 countries were defaced, and pro-Azerbaijani content was displayed.[31] In addition, controlling information on social media was an important phenomenon that DFRLab refers to as "patriotic astroturfing."[32] Financial institutions were also affected. In the period from September to November 2020, for example, as the situation in the Nagorno-Karabakh region escalated into a war (see footnote 19 for further explanation), the Central Bank of Armenia (see section "Cybersecurity Architecture - Selected Institutions") reported a surge in cyber operations. These were directed against the bank itself and other financial institutions.

The banking sector also faced various cybercrime incidents. In 2017, the operation of a cybercriminal group was uncovered, which used a Trojan known as Silence Trojan to infiltrate the systems of various banks worldwide, including in Armenia.[33] Another example is an operation discovered in November 2021 that compromised the integrity of systems of various organizations, including financial institutions in Armenia, at least since 2019.[34]

Key Documents

Several key documents shape Armenia's cybersecurity policy landscape. Among others, these include the Concept of Information Security, the Armenia 2020 National Security Strategy, Armenia's Digitization Strategy 2021-2025, and the 2018-2030 Digital Transformation Agenda of Armenia[35]

In 2009, the **"Concept of Information Security"** was adopted by order of Armenia's president.[36] The document focused mainly on the importance of information security and states "that the right of secrecy of personal data, telephone and email communication of individuals must be insured."[37] In addition, it entailed provisions on data protection.[38] Since then, the government has created a draft version of a cybersecurity strategy that is

currently being discussed under the responsibility of the Ministry of High-Tech Industry of the Republic of Armenia's Communication and Information Department (for more information, please see section "Cybersecurity Architecture - Selected Institutions"). The draft version, for example, includes plans to establish a cybersecurity center to coordinate activities in the field.[39] In 2017, the government officially announced that the strategy was ready to be submitted to Armenia's Security Council and soon to be released.[40] Until today, there is no publicly available formal version.[41]

Cybersecurity, however, gets addressed in the **National Security Strategy of the Republic of Armenia**.[42] The National Security Council approved the strategy in 2020.[43] Cybersecurity is discussed in the chapter "Ensuring Open and Safe Information and Cyber Domains," which focuses on the following topics:

- to "increase the efficiency of institutions and processes"[44] in the fields of information, technology, and cybersecurity;
- to improve the management of the sector by "introducing comprehensive mechanisms"[45];
- to develop a legal-normative framework to better "regulate the relationship between the operators of critical information infrastructure, digital service providers, and the state"[46];[3]
- to establish a national cybersecurity center and computer emergency response teams.

Cybersecurity is further mentioned in the context of hybrid warfare. As described in the strategy, hybrid warfare includes cyberattacks and other components, such as economic means and military elements.[47] The document further discusses key challenges in the field, such as the "imperfection of a comprehensive state policy regulating the information and cybersecurity sector, the absence of legislation to ensure the protection of critical information infrastructure, the insufficient level of institutional capacity of computer emergency response teams, and the absence of a national cybersecurity center."[48]

In the absence of legislation, the former Ministry of Transport, Communications and Information Technology[4] implemented **policies in the reference domain to protect critical national infrastructure against threats from cyberspace**.[49] The policies shall be implemented voluntarily by each sector's competent authorities, for example, airway and railway.[50]

Cybersecurity is also seen as an important aspect of the country's digital transformation. This is recognized by the adoption of "**Armenia's Digitization Strategy 2021-2025**"[51] in February 2021. The strategy entails nineteen activities to be implemented in two phases until

3 The National Security Strategy of the Republic of Armenia repeatedly mentions critical (information) infrastructure. However, the strategy, as well as other official and publicly available documents, do not entail a definition of infrastructures considered critical.

4 The Ministry of Transport, Communications and Information Technology is now called the Ministry of High-Tech Industry of the Republic of Armenia, according to its website (Ministry of High-Tech Industry of the Republic of Armenia (n.d.): Previous Ministers. https://hti.am/main.php?lang=3&page_id=492#)

2025 to improve digitization among the government, economy, and society. The strategy's measures aim at improving the use of digital government and e-commerce among the population, among others. Cybersecurity is one of the key areas for development.[52]

"**Armenia's Digital Transformation Agenda 2018-2030**" was developed by the Center for Strategic Initiatives and the Board of Trustees of the Digital Armenia Foundation on behalf of the Armenian government. It was officially presented and adopted in 2017. The strategic document also aims for digitization reforms in several priority areas: cybersecurity, and others, such as infrastructure.[53] For cybersecurity, the Agenda aims to move the country towards a safer and more resistant cyberspace.[54] In December 2021, after previously highlighting the importance of evaluating the Agenda's implementation, Armenia's Prime Minister stated that the results of the implementation were not as expected.[55] Therefore, he introduced a proposal to delegate more responsibilities to the Central Bank based on the banking system's interest in digital transformation. He also emphasized that cybersecurity should remain one of the main priorities of digital transformation.[56] How the Agenda relates to "Armenia's Digitization Strategy 2021-2025" is unclear based on publicly available (English) information.

Legal Frameworks

Although international cybersecurity regulations apply in Armenia, such as Armenia's adhesion to the **Convention on Cybercrime** (see chapter "Bilateral and Multilateral Cooperation"), the following section focuses solely on selected key elements of the national legal framework. These include, among others, the Criminal Code of the Republic of Armenia, the Law of the Republic of Armenia on Protection of Personal Data, and the Law of the Republic of Armenia on Electronic Communications.

The **Criminal Code of the Republic of Armenia** compiles the country's criminal law that also applies to offenses against cybersecurity and cybercrime. Chapter 24, entitled "Crimes against computer information security," explicitly defines certain forms of cybercrime, such as "Access (penetration) into computer information system without permission" (Article 251), "Computer sabotage" (Article 253), and "Manufacture, use and dissemination of hazardous software" (Article 256).[57] For other offenses, the text of the law explicitly states that the commission of the crime with the help of computers is also criminalized, for example, theft by means of a computer (Article 181) or the distribution of child pornography online (263).

The **Law of the Republic of Armenia on Protection of Personal Data**, enacted in 2015, regulates procedures and obligations for the treatment of personal data in Armenia.[58] Data processors are thereby obliged to "ensure the protection of information systems containing personal data against accidental loss, unauthorised access to information systems, unlawful use, recording, destructing, altering, blocking, copying, disseminating personal data and other interference" (Article 19). In the event of a leak of personal data, the data processor

must inform the public and the relevant state authorities (Police of the Republic of Armenia and Data Protection Authority) about the breach (Article 21). The Data Protection Agency (See chapter "Cybersecurity Architecture - Selected Institutions") is responsible for monitoring the compliance of data processors with these rules.[59]

The **Law of the Republic of Armenia on Electronic Communications,** adopted in 2005, regulates all forms of electronic communication on the Armenian territory.[60] It does not directly mention cybersecurity or information security, but its provisions contribute to protecting the integrity of electronic communications. In Article 50, the law specifies that no other person than the recipient of a message „may intercept, record, or disclose the content of such message" unless directly authorized by the involved parties or in special exemptions defined in Armenian law.[61]

Cybersecurity Architecture - Selected Institutions

Several national key actors shape Armenia's cybersecurity. These include the following governmental and non-governmental institutions, among others: the Ministry of High-Tech Industry of the Republic of Armenia, the National Security Service, the Ministry of Justice of the Republic of Armenia, the Data Protection Authority, Investigative Committee of the Republic of Armenia, the Prosecutor General's Office of Armenia, the Division for Combating High-Tech Crime at the Police of the Republic of Armenia, the Central Bank of Armenia, Armenia's national information security center, and Internet Society Armenia. More information on each stakeholder can be found below.

The **Ministry of High-Tech Industry of the Republic of Armenia** is a central body of executive authority, established in 2017, responsible for developing and implementing government policies in different areas, such as communication, information technology, information security, and the military industry.[62] The Ministry of High-Tech Industry of the Republic of Armenia is responsible for developing the cybersecurity strategy (see "Key Documents")[63] and coordinates activities related to the field of cybersecurity. It is thus, for example, responsible for the development of a common cybersecurity policy and an action plan, including, for example, the establishment of a cybersecurity center or rapid response mechanisms for emergencies. It also organizes cybersecurity awareness programs, among other tasks.[64]

The **National Security Service (NSS)** of the Republic of Armenia's functions are outlined in the Statute of the National Security Service of the Republic of Armenia, confirmed by the Prime Minister in 2018. Among other tasks, the NSS is responsible for (counter-)intelligence activities and analyzing information on threats to the country's security.[65] In regards to cybersecurity, the NSS is, for example, responsible for the protection of government infrastructure and critical infrastructure.[66] In the past, the NSS was responsible for heading a working group as outlined in the annex to the "Concept on Formation of Electronic Society

in Armenia."[5] In this role, the NSS was responsible for drafting an action plan with aspects of cybersecurity and cybercrime legislation or compliance with ISO standards.[67] In recent years, the NSS, for example, worked on public-private sector cooperation[68] and international exchange[69] in the field of cybersecurity. It further has preliminary and main functions of investigation of cybercrime.[70]

The **Ministry of Justice of the Republic of Armenia** is responsible for the legislative framework[71] and "shares organizational tasks within the government sector, regarding the codification and legal reforms."[72] Among other tasks, it is also responsible for generating informal cooperation between Armenia's public and private sectors. The Ministry of Justice further ensures compliance with the Budapest Convention on Cybercrime (see chapter Bilateral and Multilateral Cooperation)[73]. The Ministry also hosts the Data Protection Authority, depicted below.

The **Data Protection Authority (DPA)**, established in 2015, is Armenia's main regulatory authority for data protection, with binding authority on public and private institutions.[74] The DPA is supervised by the government[75] and hosted by the Ministry of Justice.[76] Its tasks are, among others, to ensure the "maintenance of the register of personal data processors,"[77] the "protection of the rights of the subjects related to the protection of personal data,"[78] and the "legality of the processing of personal data within its competence."[79] The DPA, and its Commissioner, can "receive complaints or open an investigation at its own initiative."[80] It also has the authority to impose fines when regulations are breached.[81]

Since 2011, the **Investigative Committee of the Republic of Armenia**[82] has been responsible for investigating a majority of criminal cases in Armenia. Naturally, this also entails cases of cybercrime that dedicated investigators handle. The usual investigation process starts with the investigator filing a criminal case with the prosecutor and afterward leading the investigative procedures. In this context, forensic expertise is acquired externally. The Investigate Committee signed a Memorandum of Understanding with Internet Service Providers in 2015, focusing, for example, on standardized communication between each other or developing "mutual cooperation for introducing technical capabilities."[83]

The **Prosecutor General's Office of Armenia** has certain responsibilities in the field of cybercrime, to which two prosecutors are dedicated specifically.[84] Among its tasks is to control and supervise investigative procedures "by all investigative entities in Armenia and support the criminal proceedings in case of corresponding investigations through the entire country."[85] The Prosecutor General's Office can, therefore, verify if investigations are applied lawfully, and apply actions against the investigative unit, if there is wrongdoing. In addition

5 The "Concept on Formation of Electronic Society in Armenia" was approved by the government in 2010. It set out to develop and implement a national broad-ringed network and to increase international ways of communication. Overall, the concept aimed at making online electronic management and trade-advertising services available to citizens established through a private sector-state cooperation investment scheme. (ARMENPRESS (2010): Armenian government approves the concept on formation of electronic society in Armenia. https://bit.ly/3qrQBnU;
The Government of the Republic of Armenia (2010): ՀԱՅԵՑԱԿԱՐԳ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆՈՒՄ ԷԼԵԿՏՐՈՆԱՅԻՆ ՀԱՍԱՐԱԿՈՒԹՅԱՆ ՁԵՎԱՎՈՐՄԱՆ (2010-2012ԹԹ.). https://armcci.am/files/E-society%20Development%20Concept%20Paper.pdf).

to these tasks, it also plays a crucial part in international cooperation on cybercrime, for example, with Interpol. On the national level, the Prosecutor General's Office cooperates with Internet Service Providers (ISPs), among others.[86]

The centralized police unit **Division for Combating High-Tech Crime** at the **Police of the Republic of Armenia**, operating under the General Department on Combating Organized Crime, is responsible for handling cybercrime cases before official investigations are opened with "country-wide competency".[87] The unit investigates "offences committed against computer systems such as hacking, attacks on critical infrastructure, illegal interception and data interference"[88] as well as "offences involving technology such as computer related fraud, Internet crimes, offences involving the abuse of children, intellectual property offences as well as racism and xenophobia."[89] Within a set time frame of ten days, the Division for Combating High-Tech Crime can either decide to close the case or to transfer it to another entity, such as the NSS, the local police, or the Investigative Committee.[90] In the past, the Division has, for example, worked with the Organization for Security and Co-operation in Europe (OSCE) (see section "Bilateral and Multilateral Cooperation" below) to organize a conference on cybercrime.[91]

The **Central Bank of Armenia (CBA)** aims to maintain price and financial stability by developing and implementing monetary policy, according to its last published institutional strategy 2018-2020.[92] Armenia's financial system, which includes the banking system, is regulated by the CBA. In accordance with international developments, Armenian banks now offer digital services, such as online and mobile banking. In the field of cybersecurity, CBA's representatives have publicly highlighted the importance of addressing cybersecurity risks in the financial sector as well as the importance of defending against such risks.[93] In 2018, the CBA and the Bank of Russia signed an information security cooperation agreement. Both countries' national regulators agreed on exchanging information about cyber incidents, aiming at preventing, detecting, and countering them. The banks agreed to notify each other in the case of cyber incidents. In addition, the cooperation contains an agreement to "carry out a comprehensive analysis of such information and deliver the results to the other Party,"[94] if technologically feasible, or forward information on incidents to the other party for further analysis.[95]

Armenia's national information security center is called **CERT AM/AM NREN CSIRT**. It consists of the national Computer Emergency Response Team (CERT-AM), administered by the Armenian Internet domain, and the Armenia National Research and Education Network Computer Security Incident Response Team, the AM NREN CSIRT, administered by the Academic Scientific Research Computer Network of Armenia. The CERT AM/AM NREN CSIRT is managed by the Internet Society of Armenia (please see below for more information), and can, therefore, be considered a non-governmental institution. Its responsibilities entail collecting information about computer incidents affecting networks located in Armenia, analyzing them as well as potential responses.[96] In addition, it serves as a point of contact "for users who need an assistance in dealing with ISPs and Armenian official bodies which are in charge for investigating computer crime cases."[97] In the past, the CERT-AM has thus, for ex-

ample, cooperated with the National Police of Armenia "in handling cybersecurity incidents and provides support in cybercrime cases."[98]

In addition to the (governmental) institutions mentioned, there are other private sector and civil society institutions active in the field of cybersecurity. Among these institutions, for example, is the Internet Society (ISOC) Armenia, also called the "Internet Society" NGO. The Internet Society Armenia manages Armenia's CERT AM/AM NREN CSIR, as explained above, and therefore, has a vital role in Armenia's cybersecurity landscape. ISOC Armenia's main objective is to promote internet development in the country. As the Secretariat of the Internet Governance Council, it is further responsible for the organization of the Armenian Internet Governance Forums, among others. It maintains cooperation with the Ministry of High-Tech Industry of the Republic of Armenia, established in a common Memorandum of Understanding.[99]

Generally, there is continuous public-private sector dialogue in cybersecurity, for example, when representatives of the private sector are invited to the Parliament's committees to speak on the topic.[100]

Bilateral and Multilateral Cooperation

In regard to multilateral cooperation, Armenia is a member of several international organizations, such as the United Nations (UN) and the International Telecommunication Union (ITU), among others, that work on topics related to cybersecurity. Besides engaging in different dialogue and cooperation (see below), Armenia also cooperates bilaterally with other countries in this area. Key areas of cooperation on the multilateral and bilateral levels are the prevention and prosecution of cybercrime as well as cyber defense.

As a member of the **United Nations** (UN), Armenia participated actively in the **Open-ended working group on developments in the field of information and telecommunications in the context of international security** (OEWG). In its two comments on drafts of the OEWG report, Armenia suggested that states should commit to refrain from taking actions that could damage or disrupt critical infrastructure.[101] Additionally, the UN and Armenia agreed on the United Nations Sustainable Development Cooperation Framework for Armenia (2021-2025). One goal of this framework is to enhance the cybersecurity skills in the Armenian population by, among other aspects, "promoting civic education" and "supporting women and girls in STEM."[102] Armenia has also been a member of the **International Telecommunication Union** (ITU) since 1992.[103] The ITU aims to strengthen international cooperation, enhance the security of and confidence in ICTs, and provide necessary information to member states.[104]

The fight against cybercrime is a crucial component of Armenia's cooperation with multilateral partners. Armenia has publicly demonstrated its commitment to this issue by signing (2001) and ratifying (2006) the **Convention on Cybercrime (Budapest Convention)**, which aims to harmonize cybersecurity and cybercrime legislation and strengthen international cooperation in this area.[105]

The **Comprehensive and Expanded Partnership Agreement**, agreed on by the European Union and Armenia, entered into force in March 2021. It commits both actors to cooperate in foreign and security policy, particularly in cybersecurity, and cooperation in combating and preventing cybercrime by enhancing "bilateral, regional and international cooperation among law-enforcement bodies."[106] This focus on preventing and combating cybercrime is also reflected in other collaborations in the EU context, such as the recently signed **Strategic Cooperation Agreement** with **Europol**. Both partners commit to strengthening cooperation in combating different forms of cross-border crime, including cybercrime.[107] Another example is the **CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern partnership region**, a joint project of the EU and the Council of Europe and part of the EU4Digital initiative.[108] The main objective of CyberEast is to implement legislation consistent with the provisions of the Budapest Convention (please see above) in the target countries, including Armenia, and other measures to strengthen the fight against cybercrime.[109] Additional projects with a similar focus on improving cooperation on cybercrime in the Eastern Partnership countries have existed since 2011.[110] Additionally, the CyberEast project includes other goals in the field of cybersecurity, such as the development of improved incident response procedures.[111] In addition to the CyberEast project, EU4Digital also supports the development of e-government solutions in Armenia.[112]

The fight against cybercrime is also an essential aspect of cooperation with the **Organization for Security and Co-operation in Europe (OSCE)**. At least since 2007, the organization has been actively collaborating with the Armenian authorities in this area.[113] Currently, the extrabudgetary project **Capacity Building on Combating and Preventing Cybercrime in Armenia**, funded mainly by Germany, aims to enable Armenian law enforcement agencies to better prosecute cybercrime by offering training and guidelines.[114]

The cooperation with collective defense and security organizations, such as the **Collective Security Treaty Organization** (CSTO) and the **North Atlantic Treaty Organization** (NATO), has a slightly different focus. Armenia was a member of the CSTO since its foundation in 2003 and also adhered to the predecessor Collective Security Treaty.[115] The CSTO considers the protection of the so-called infosphere "the most important area of the system of collective security."[116] One of its measures is the establishment of the Consultative Coordination Center for Computer Incident Response (CSTO CCC), which furthers cooperation among treaty members to facilitate joint measures in cases of computer incidents.[117]

Armenia has been a member of the North Atlantic Cooperation Council (later renamed the Euro-Atlantic Partnership Council) since 1992. Several Individual Partnership Action Plans (IPAP)[6] now structure joint cooperation in defense and beyond.[118] Concrete measures for the period 2014-2016, for example, included the establishment of response procedures to identify cyber threats or the harmonization of the national legal framework with international standards.[119]

6 With the publicly available sources used, this research could not conclusively clarify whether NATO and Armenia have agreed on a further IPAP after the IPAP 2017-2019.

Armenia also works together with other states on a bilateral level. Armenia, for example, signed an agreement on military cooperation, including a focus on cyber defense, with France in 2018[120]. In addition, it is currently drafting a cyber security cooperation agreement with Russia.[121] Partners such as the United States agreed on projects to support the development of cybersecurity awareness among the population, in addition to previously mentioned projects with multilateral partners[122] and institutional cooperation agreements, such as the information security cooperation agreement between the Central Bank of Armenia and the Bank of Russia (please see “Cybersecurity Architecture - Selected Institutions”).

Sources

1 Embassy of Armenia to the United States of America: General information about Republic of Armenia. https://usa.mfa.am/en/overview/

2 Embassy of Armenia to the United States of America: General information about Republic of Armenia. https://usa.mfa.am/en/overview/

3 The Government of the Republic of Armenia (2022): Demographics. https://www.gov.am/en/demographics/

4 The Ministry of Foreign Affairs of the Republic of Armenia: General information about Republic of Armenia. https://www.mfa.am/en/overview

5 Embassy of Armenia to the United States of America: General information about Republic of Armenia. https://usa.mfa.am/en/overview/

6 Aleksandrovich Mints and Howe (2022): Government and society. https://www.britannica.com/place/Armenia/Government-and-society

7 The Government of the Republic of Armenia (2022): State administration system. https://www.gov.am/en/gov-system/

8 The President of the Republic of Armenia (2022): Vahagn Khachaturyan assumed office as the President of the Republic of Armenia at the special sitting of the RA National Assembly. https://bit.ly/3JADNDc

9 The Prime Minister of the Republic of Armenia (2021): Biography. https://www.primeminister.am/en/pm-pashinyan

10 The Government of the Republic of Armenia (2022): State administration system. https://www.gov.am/en/gov-system/

11 The Government of the Republic of Armenia (2022): State administration system. https://www.gov.am/en/gov-system/

12 The Government of the Republic of Armenia (2022): State administration system. https://www.gov.am/en/gov-system/

13 World Bank Group (2017): Future Armenia: Connect, Compete. Prosper - A Systematic Country Analysis. https://bit.ly/3tZVWUn

14 World Bank Group (2017): Future Armenia: Connect, Compete. Prosper - A Systematic Country Analysis. https://bit.ly/3tZVWUn

15 World Bank Group (2017): Future Armenia: Connect, Compete. Prosper - A Systematic Country Analysis. https://bit.ly/3tZVWUn

16 Statistical Committee of the Republic of Armenia (2019): Armenia - Poverty Snapshot over 2008-2018. https://armstat.am/file/article/poverty_2019_e_2.pdf

17 The International Bank for Reconstruction and Development (2018): Connecting to Compete 2018. https://openknowledge.worldbank.org/bitstream/handle/10986/29971/LPI2018.pdf

18 Government of the Republic of Armenia (2021): (ՀԱՅԱՍՏԱՆԻ ԹՎԱՅՆԱՑՄԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆ 2021-2025. https://www.arlis.am/DocumentView.aspx?docID=149957

World Bank (2022): Armenia to Improve Public Sector Performance through Digital Solutions, with World Bank Support. https://bit.ly/37Xs9Vj

19 Agence Française de Développement (2022): Armenia. https://www.afd.fr/en/page-region-pays/armenia

20 World Bank Group (2021): Competition and Firm Recovery Post-COVID-19. https://bit.ly/37neUwz

World Bank (2021): The World Bank in Armenia. https://www.worldbank.org/en/country/armenia/overview#1

21 Freedom House (2022): Armenia. https://freedomhouse.org/country/armenia/freedom-net/2021#footnote3_n2z0y84

22 Reporters without Borders (2021): Diversity but not yet independence. https://rsf.org/en/armenia

23 Reporters without Borders (2021): Diversity but not yet independence. https://rsf.org/en/armenia

24 Freedom House (2022): Armenia. https://freedomhouse.org/country/armenia/freedom-net/2021#footnote3_n2z0y84

25 World Economic Forum (2019): The Global Competitiveness Report 2019. https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

26 FireEye (2014): APT28: A Window into Russia's Cyber Espionage Operations?. https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

Paganini (2020): Russia-Linked Turla APT uses new malware in watering hole attacks https://bit.ly/3KWJSKA

Secure List (2013): "Red October" Diplomatic Cyber Attacks Investigation. https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#8

27 Citizen Lab (2017): Tainted Leaks. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

28 Secure List (2013): "Red October" Diplomatic Cyber Attacks Investigation. https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#8

29 FireEye (2014): APT28: A Window into Russia's Cyber Espionage Operations?. https://www2.fireeye.com/rs/fireye/images/rpt-apt28.pdf

30 Martirosyan (2018): Armenia at the Center of State-Sponsored Cyber Attacks. https://evnreport.com/politics/armenia-at-the-center-of-state-sponsored-cyber-attacks/

31 Hackread (2016): Azerbaijani Hackers Deface NATO-Armenia, Embassy Websites in 40 Countries. https://www.hackread.com/azerbaijani-hackers-defac-nato-armenia-embassy-sites/

32 DFRLab (2020): Patriotic astroturfing in the Azerbaijan-Armenia Twitter war. https://bit.ly/3N6h3gP

33 Secure List (2017): Silence - a new Trojan attacking financial organizations. https://securelist.com/the-silence/83009/

34 Central Bank of Armenia (2021): Annual Report 2020. https://www.cba.am/EN/pperiodicals/Annual%20report_2021.pdf

Yamout (2021): WIRTE's campaign in the Middle East 'living off the land' since at least 2019. https://bit.ly/3Ihjqtt

35 UNIDIR (2021): Armenia. https://cyberpolicyportal.org/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiMTkxIn0

36 ARLIS (2017): ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԱՅԵՑԱԿԱՐԳԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ. https://www.arlis.am/DocumentView.aspx?docID=52559

37 Grigoryan (2018): Cyberspace in Armenia: Limitations and Cases of Cyber Security Violations. https://en-gmr.mapn.ro/app/webroot/fileslib/upload/files/grigoryan.pdf

38 Grigoryan (2018): Cyberspace in Armenia: Limitations and Cases of Cyber Security Violations. https://en-gmr.mapn.ro/app/webroot/fileslib/upload/files/grigoryan.pdf

39 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

Ministry of High-Tech Industry (2017): ՀՀ կառավարության «Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ. https://www.e-draft.am/en/projects/581/about

Ministry of High-Tech Industry (2017): ՀՀ կառավարության «Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ. https://www.e-draft.am/en/project/download/pdf?id=581

Elamiryan (2021): Armenian National Policy in Cyber Space. https://bit.ly/3IrGMfW

40 ARMENPRESS (2017): Armenia's cybersecurity strategy document is ready. https://bit.ly/3Ju4vNQ

41 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

42 The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

43 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

44 The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

45 The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

46 The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

47 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

48 The Government of the Republic of Armenia (2020): National Security Strategy Of The Republic Of Armenia. https://bit.ly/3IwzPdB

49 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

50 European Union and the Council of Europe (2019): Cybercrime and cybersecurity strategies in the Eastern Partnership region. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

51 Government of the Republic of Armenia (2021): (ՀԱՅԱՍՏԱՆԻ ԹՎԱՅՆԱՑՄԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅՈՒՆ 2021-2025. https://www.arlis.am/DocumentView.aspx?docID=149957

52 The World Bank (2021): South Caucasus GovTech for Armenia A Whole of Government Approach as a Key Foundation for the Digital Economy in Armenia. https://bit.ly/3D4ZGYP

Ghazanchyan (2021): Armenia to go digital as government approves new strategy. https://en.armradio.am/2021/02/11/armenian-government-approves-the-digitalization-strategy/

53 The Government of the Republic of Armenia (2017): Armenia Digital Agenda - 2030 Long-Term Strategy Presented. https://www.gov.am/en/news/item/9211/

54 The Government of the Republic of Armenia (2018): Draft Framework Paper on 2018-2030 Digital Transformation Agenda Submitted for Discussion. https://www.gov.am/en/news/item/9307/

55 ARKA Telecom (2021): Pashinyan: we have quite a large digital agenda, but we do not have results. https://bit.ly/3twRkWP

ARMENPRESS (2021): Implementation of Armenia's digital agenda strategy discussed at Government. https://armenpress.am/eng/news/1061121.html

56 ARKA Telecom (2021): Pashinyan: we have quite a large digital agenda, but we do not have results. https://bit.ly/3twRkWP

57 National Assembly of the Republic of Armenia (2021): Criminal Code of the Republic of Armenia. http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=eng

58 Freedom of Information Center of Armenia (2015): Law of the Republic of Armenia on Protection of Personal Data http://www.foi.am/u_files/file/Personaldataprotection-law_ENG.pdf

59 Ministry of Justice of the Republic of Armenia (2016): Statute of the Agency for Protection of Personal Data of the Ministry of Justice of the Republic of Armenia https://moj.am/en/structures/view/structure/32

60 Armenian Legal Information System (2005): Law of the Republic of Armenia on Electronic Communications. https://www.arlis.am/Annexes/4/elektr_com_en.pdf

61 Armenian Legal Information System (2005): Law of the Republic of Armenia on Electronic Communications. https://www.arlis.am/Annexes/4/elektr_com_en.pdf

62 The Government of the Republic of Armenia (n.d.): Ministry of High-Tech Industry. https://www.gov.am/en/structure/277/

EU4Digital (n.d.): Armenia. https://eufordigital.eu/countries/armenia/

63 Ministry of High-Tech Industry (2017): ՀՀ կառավարության «Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ. https://www.e-draft.am/en/projects/581/about

Ministry of High-Tech Industry (2017): ՀՀ կառավարության «Կիբեռանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ. https://www.e-draft.am/en/project/download/pdf?id=581

64 The Government of the Republic of Armenia (2019): ՀԱՅԱՍՏԱՆԻ ԹՎԱՅՆԱՑՄԱՆ ՌԱԶՄԱՎԱՐՈՒԹՅԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԻ ԾՐԱԳԻՐԸ ԵՎ ԱՐԴՅՈՒՆՔԱՅԻՆ ՑՈՒՑԱՆԻՇՆԵՐԸ.

65 National Security Service of the Republic of Armenia (n.d.): Functions. https://www.sns.am/en/functions/

National Security Service of the Republic of Armenia (n.d.): Goals and main objectives.https://www.sns.am/en/goals-and-main-objectives/

66 European Union and the Council of Europe (2019): Cybercrime and cybersecurity strategies in the Eastern Partnership region. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

67 European Union and the Council of Europe (2019): Cybercrime and cybersecurity strategies in the Eastern Partnership region. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

68 National Security Service of the Republic of Armenia (2018): The National Security Service will contribute to the cyber security of Armenia. https://bit.ly/3L6U9E5

69 National Security Service of the Republic of Armenia (2019): Issues Related to Fight Against New Challenges of International Terrorism Discussed in Sochi. https://bit.ly/3IzYVs1

70 Republic of Armenia (2021): ՕՐԵՆՔԸ ՔՐԵԱԿԱՆ ՕՐԵՆՍԳԻՐՔ. http://parliament.am/legislation.php?sel=show&ID=7645&lang=arm#12.38

71 Council of Europe (n.d.): The Ministry of Justice of Armenia. https://www.coe.int/en/web/cybercrime/ministry-of-justice-dpa-am

Ministry of Justice of the Republic of Armenia (2018): Charter of the Ministry of Justice of the Republic of Armenia. https://www.moj.am/en/page/statute

72 Council of Europe (n.d.): The Ministry of Justice of Armenia. https://www.coe.int/en/web/cybercrime/ministry-of-justice-dpa-am

MOJ (n.d.): Ministry of Justice of the Republic of Armenia. https://www.moj.am/en

73 Council of Europe (n.d.): The Ministry of Justice of Armenia. https://www.coe.int/en/web/cybercrime/ministry-of-justice-dpa-am

74 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

75 Margaryan, Abrahamyan, and Hovhannesyan (2021): Armenia - Data Protection Overview Introduction. https://www.dataguidance.com/notes/armenia-data-protection-overview

76 Council of Europe (n.d.): The Ministry of Justice of Armenia. https://www.coe.int/en/web/cybercrime/ministry-of-justice-dpa-am

77 Margaryan, Abrahamyan, and Hovhannesyan (2021): Armenia - Data Protection Overview Introduction. https://www.dataguidance.com/notes/armenia-data-protection-overview

MOJ (n.d.): Ministry of Justice of the Republic of Armenia. https://www.moj.am/en

78 Margaryan, Abrahamyan, and Hovhannesyan (2021): Armenia - Data Protection Overview Introduction. https://www.dataguidance.com/notes/armenia-data-protection-overview

79 Margaryan, Abrahamyan, and Hovhannesyan (2021): Armenia - Data Protection Overview Introduction. https://www.dataguidance.com/notes/armenia-data-protection-overview

80 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

81 DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

82 Investigative Committee of the Republic of Armenia (n.d.): Investigative Committee of the Republic of Armenia. https://www.investigative.am/en/home.html

83 Council of Europe (2020): Armenia. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[1]}

84 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[2]}

The Prosecutor General's Office of the RA (n.d.): .The Prosecutor General's Office of the RA. https://www.prosecutor.am/en/noexists/

DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

85 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#%7B%22105470988%22:[2

86 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#%7B%22105470988%22:[2

DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

87 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[0]}

Police of the Republic of Armenia (n.d.): Police of the Republic of Armenia. https://www.police.am/en/home.html

88 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[0]}

89 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[0]}

90 Council of Europe (2020): Armenia Institutions. https://www.coe.int/en/web/cybercrime/institutions_am#{%22105470988%22:[0]}

Republic of Armenia (2021): ՕՐԵՆՔԸ ՔՐԵԱԿԱՆ ՕՐԵՆՍԳԻՐՔ. http://parliament.am/legislation.php?sel=show&ID=7645&lang=arm#12.38

91 Police of the Republic of Armenia (2011): Ընդդեմ կիբերհանցավորության http://old.police.am/news/view/ընդդեմ-կիբերհանցավորության.html

92 The Central Bank of the Republic of Armenia (2020): Strategy 2018-2020. https://www.cba.am/EN/panalyticalmaterialsresearches/Strategy_2018.2020.pdf

93 GCAP (2019): Addressing Cyber Security Risks in Emerging Financial Sectors. https://www.cgap.org/node/4211

Stepanyan (2019): Cyber Security Risks For Central Banks in Emerging and Developing Countries. https://www.cgap.org/sites/default/files/event_documents/2019_11_Setting_Stage.pdf

94 Bank of Russia (2018): Bank of Russia and Central Bank of Armenia make information security cooperation agreement. http://www.cbr.ru/eng/press/event/?id=2103

95 Bank of Russia (2018): Bank of Russia and Central Bank of Armenia make information security cooperation agreement. http://www.cbr.ru/eng/press/event/?id=2103

96 CERT-AM (n.d.): About Us. https://www.cert.am/

DCAF, Spînu (2020): Armenia Cybersecurity Governance Assessment. https://bit.ly/3D1VU2F

97 CERT-AM (n.d.): About Us. https://www.cert.am/

98 Council of Europe (n.d.): Computer Security Incident Response Team of Armenia CERT.AM. https://www.coe.int/en/web/cybercrime/cert-am

99 ISOC.am (n.d.): Main activity. https://www.isoc.am/en/what-we-do/main-activity/

100 European Union and the Council of Europe (2019): Cybercrime and cybersecurity strategies in the Eastern Partnership region. https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c

101 Armenia (2020): On the initial pre- draft of the report of the OEWG on the developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2020/04/nonpaper-4-oewg-report.doc.pdf

Armenia (2021): Proposal on the Zero and First draft. https://front.un-arm.org/wp-content/uploads/2021/02/Armenia.pdf

102 United Nations Armenia (2021) : United Nations Sustainable Development Cooperation Framework for Armenia. https://bit.ly/3teXb2R

103 ITU (2022): List of Member States. https://www.itu.int/online/mm/scripts/gensel8

104 ITU (n.d.): ITU Cybersecurity Activities. https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

105 Council of Europe (2020): Armenia. https://www.coe.int/en/web/cybercrime/institutions_am

106 European Union (2018): Comprehensive and Enhanced Partnership Agreement. https://bit.ly/34M1rh3

107 Europol (2021): Armenia and Europol sign agreement to combat cross-border serious organised crime. https://bit.ly/3IfyUy5

108 The European Union for Armenia (2020): CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region. https://eu4armenia.eu/projects/eu-project-page/?id=716

109 Council of Europe (2022): CyberEast Fact Sheet. https://rm.coe.int/cybereast-fact-sheet-march22/1680a5cc24

110 Council of Europe (2016): Project Cybercrime@EAP III. https://rm.coe.int/3608-ceapiii-summary-workplan-/1680758af4

111 EU4Digital (n.d.): CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region. https://bit.ly/3q8U1vw

112 EU4Digital (n.d.): Armenia. https://eufordigital.eu/countries/armenia/

113 OSCE (2007): OSCE Office in Yerevan assists Armenia in improving cyber security. https://www.osce.org/yerevan/48767

114 OSCE (2021): OSCE trains law enforcement and criminal justice officials in Armenia on combating and preventing cybercrime. https://www.osce.org/secretariat/509366

115 CSTO (2018): The Republic of Armenia. https://en.odkb-csto.org/countries/armeniya/

116 CSTO (2020): Speech of the CSTO Deputy Secretary General Valery Semerikov at the meeting of the heads of national staffs of the CSTO member states on the operation "PROXY" on March 13, 2020. https://bit.ly/3if96rj

117 CSTO (2021): The XII meeting of the Council of the CSTO Consultative Coordination Center for Computer Incident Response was held. https://bit.ly/3tfi661

118 Ministry of Foreign Affairs of the Republic of Armenia (2019): International organisations. https://www.mfa.am/en/international-organisations/3

119 Elamiryan (2021): Armenian national policy in cyber space. https://www.routledgehandbooks.com/doi/10.4324/9780429399718-3

120 Papazian (2019): La Francophonie, un atout stratégique dans la diplomatie de défense de l'Arménie. https://bit.ly/3i99jMA

121 Ghazanchyan (2022): Armenia, Russia draft agreement on cooperation in cyber security. https://bit.ly/3MUEvNW

122 USAID (2020): USAID and Armenia: Partners since 1992. https://bit.ly/3JaCMlb