PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NO. 5 (191), FEBRUARY 2021 © PISM

Editors: Sławomir Dębski, Patrycja Sasnal, Wojciech Lorenz

Boosting Cybersecurity Resilience in the Eastern Partnership Region: Options for the EU

Elżbieta Kaca

Cyberattacks coupled with online disinformation campaigns are an increasing threat in Eastern Partnership (EaP) countries, while their capacities to counter it are limited. At the forthcoming EaP summit in 2021, the EU could offer a new cybersecurity package for its partners. The EU might deepen political cooperation with associated countries through cyber dialogues and develop aid programmes for the protection of critical infrastructure and enhanced interagency cooperation. Regionally, the EU could better counter disinformation by strengthening East StratCom and increasing support for media literacy and critical thinking among youth.

The COVID-19 pandemic has significantly increased cybersecurity threats due to the greater use of teleworking and digitisation of public services and social life[1]. Conventional cybercrime such as thefts or cyberbullying have increased, while cyberattacks committed by state-related actors have become more sophisticated.[2] The use of the newest technologies has made cyberespionage, attacks on critical infrastructure,[3] and disinformation through social media harder to detect. The development of artificial intelligence (AI) will only deepen this trend. It could potentially enable more efficient attacks on networks as well as speedy dissemination of false information through the use of language processing models or deep fakes—video or audio creations that purport to be real.

In response, the EU wants not only to enhance operational and intelligence cooperation between Member States in the field of cybersecurity but also to strengthen cooperation with third countries, namely those in the Western Balkans and the EU's eastern and southern neighbourhoods. According to the Cybersecurity Strategy[4] adopted in December 2020, the EU plans to expand cyber dialogues with some countries and develop capacity-building programmes. The EU's greater cybersecurity ambition gives a chance to develop collaboration between the Union and EaP countries in this respect.

Cyber Threats and Systemic Gaps in the EaP Region

Cyber threats pose a significant danger to the security of the Eastern Partnership countries. The highest risk of state destabilisation is connected to politically motivated cyberattacks pursued by state-sponsored actors (Table 1). These might involve spying on confidential political and economic information, impacting electoral processes, distorting critical infrastructure networks (e.g., in transport, banking, communications, energy), or even undermining defence capabilities during a military confrontation. The majority of cyberattacks in the EaP region is affiliated with Russia, with Chinese and Turkish hacker groups detected to a lesser extent.[5] So far, while the whole EaP region has been suffering from cyberespionage, the countries most exposed to cyberattacks have been Georgia and Ukraine due to their direct military confrontation with Russia. The latter has been a test case for Russian cyber operations. The first-ever cyberattack on a power grid was committed in Ukraine in 2015 and intrusions into elections-related institutions took place in 2014.

The highest risk of state destabilisation is connected to politically motivated cyberattacks pursued by state-sponsored actors.

The majority of cyberattacks in the EaP region is affiliated with Russia.

1 The scope of this paper is limited to EU actions in relation to cyber-enabled threats as part of hybrid threats in the EaP region. It does not cover the EU digital agenda.

2 "ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected" (press release), European Union Agency for Cybersecurity, October 2020, www.enisa.europa.eu.

3 Facilities, systems, sites, information, people, networks, and processes necessary for a country to function and upon which daily life depends, including such sectors as: energy, government, health, finance, food, transportation, and water.

4 "The EU's Cybersecurity Strategy for the Digital Decade," European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 16 December 2020, JOIN(2020) 18 final, www.ec.europa.eu.

5 N. Popescu, S. Secrieru, "Hacks, leaks and disruptions—Russian cyber strategies," EU ISS Chaillot Paper No. 148, October 2018, www.iss.europa.eu.

Table 1. Major Cyberattacks in the EaP Region

Ukraine

2014 - during Russia's **annexation of Crimea**, some digital infrastructure was destroyed by the Russian military; disinformation operations and electronic warfare were carried out.

April/May 2014 – during the presidential elections, **the Ukrainian Central Election Committee** network was penetrated with espionage malware, rendering it unable to receive and process election material or to announce results on time.

December 2015 - **power grid**: about 230,000 Ukrainians were without electricity for up to six hours.

December 2016 - **disruption of critical infrastructure**: Kyiv's power grid was knocked offline, Kyiv airport operations disrupted, and internal state finance institutions and telecommunication networks were paralysed.

June 2017 - **NotPetya ransomware**: 10% of computers in Ukraine were disabled (government and private companies); the ransomware spread worldwide through international firms and cost at least $10 billion to clean up.

2019 – ahead of the presidential elections, around 9,000 incidents were detected involving **ICT infrastructure of institutions responsible for holding elections**. Unlike 2014, however, there was no major impact due to efficient monitoring systems.

Georgia

2008 – during the **Russo-Georgian war**: advanced **cyberespionage on state networks** resulted in security issues; nearly 90% of state websites were attacked.

2011 - **political news-related portals and government websites** were targeted along with complex espionage intrusions onto journalists' computers.

2019 - more than 2,000 private, state, and media **websites** (i.e., TV broadcasters) **went offline** for two days.

Nagorno-Karabakh

2020 – both Armenia and Azerbaijan conducted cyberattacks on the other's **state and media websites**, supported by advanced information warfare, mainly on social media.

2020 - **PoetRAT malware** targeted government and critical infrastructure to collect intelligence—deployed against Azerbaijan.

Belarus

July 2016 - **defence industries** in Russia, **Belarus**, and Mongolia were targeted by a Chinese cyber-espionage group using phishing campaigns to extract data.

Moldova

2016 - in the run-up to the presidential elections, there were large-scale cyberattacks **on government entities, Central Election Commission websites, observation missions, and media outlets**.

Source: Own compilation based on NATO Cooperative Cyber Defence Centre of Excellence and Centre for Strategic and International Studies data and media reports.

An increasing trend in the EaP region is the dissemination of online disinformation sponsored by Russia and China.

An increasing trend in the EaP region is the dissemination of online disinformation sponsored by Russia and China.[6] Chinese disinformation efforts recently have primarily focused on the COVID-19 response. China has utilised the pandemic to try to improve its public image and maximise its vaccine diplomacy. Russian disinformation is a more serious threat to the EaP countries as its goal is to induce polarisation within societies, decrease citizens' trust in state institutions and undermine countries' alignment with the West. Russian tactics include disseminating false news, sparking rumours, or astroturfing debates on controversial topics related to values and identity. They are posted by trolls and bots on social media, an important source of information in the majority of EaP countries (e.g., Facebook, Telegram, YouTube), but also on supposedly alternative news websites pretending to be legitimate and independent sources of information, such as OneWorld.Press. A specific challenge for the EU is false narrative that Europe will politically abandon the EaP region, a claim currently repeated in Armenia since the recent flare-up in the Nagorno-Karabakh conflict. To illustrate the impact of disinformation related to COVID-19, in October 2020 around 43% of Moldovans believed that the coronavirus was developed to insert into microchips that would allow an alleged "World Government" to control humanity.[7]

Importantly, some EaP countries employ cyberattacks and disinformation themselves. Armenia and Azerbaijan both used such tools in the conflict over Nagorno-Karabakh. In authoritarian states, this weapon is used in the confrontation between the authorities and civil society. For example, during the Belarusian political crisis that began in 2020, the government has blocked people from accessing social media accounts and disrupted internet providers, while on the other side, a citizens' group called the Cyber Partisans perpetrated cyberattacks against state sites to collect data of officials responsible for the repressions.

Besides state actors, conventional cybercrime also poses a severe hazard to EaP societies in general. Such crime consists mainly of the theft of financial resources, commercial trade secrets, and personal data, along with blackmail, disruptions generating high costs, and various forms of online sexual and gender-based violence. Due to the high level of IT education and existence of grey zones in conflict territories, the EaP region is a point of operation for cybercriminals targeting the EU, mainly when it comes to sophisticated payment fraud.[8] Criminals usually hack the email accounts of employees by using social engineering tactics, such as pretending to be a director or a supplier asking for payments. Moreover, many dark markets enabling illegal transactions on anything from pharmaceuticals to firearms originate from the EaP region. For instance, in January 2021, Darkmarket, an illegal dark web marketplace operating from servers located in Ukraine and Moldova, was taken offline. It enabled trade in drugs, stolen credit card details, and malware and estimated to have generated about €140 million in turnover.[9]

EaP Countries Cybersecurity Capacities and Gaps

The capacities of the EaP countries to respond to cyberattacks varies. According to international indexes (Table 2), the most advanced country in terms of cybersecurity legislation and institutional development is Georgia, followed by Ukraine, and then Moldova. The others rank low on this list.

6 See the analysis of Russia disinformation provided by EUvsDisinfo, www.euvsdisinfo.eu.

7 "Evolution in perceptions of COVID-19 pandemic misinformation and population's political preferences," Republic of Moldova, October 2020, www.watchdog.md.

8 "Internet organised crime threat assessment (IOCTA) 2020," Europol report, 5 October 2020, www.europol.europa.eu.

9 "Darkmarket: world's largest illegal dark web marketplace taken down" (press release), Europol, 12 January 2021, www.europol.europa.eu.

Georgia and Ukraine, the most exposed in the EaP to state-sponsored cyberattacks have had the highest motivation to strengthen their security mechanisms. However, their real defensive and offensive potential to counter cyberattacks is hard to assess because the states' capabilities are secret. It seems that Ukraine is the most effective in this respect due to higher exposure to cyberthreats and the strongest IT sector in the EaP. For instance in 2018, the Ukrainian authorities claimed that they blocked several attempts by Russian hackers to disrupt judicial authorities, state agencies, banks, energy companies, and a chlorine production plant.[10] Georgia, which has a less-developed IT sector, did not manage to mitigate attacks on state and media websites in 2019.

The capacities of EaP countries to counter disinformation are also difficult to measure and no internationally recognised indexes have been developed yet. In the EaP region, Ukraine and Georgia have acknowledged disinformation as a security threat and have built up respective institutional structures and adopted some legal solutions. However, Russia's high investments in disinformation operations as well as its wide presence online and in the telecommunications sector in the EaP region, for example, in Ukraine make countering it difficult. Importantly, low media literacy among the society is an enabling factor for spreading disinformation. Moreover, despite the existence of many civil-society organisation (CSO) that conduct fact-checking, major online news and social media platforms are unwilling to cooperate with them as it is simply too a small market to bother. The cross-platform distribution of false news also significantly complicates the efforts to counter it.

The low level of general awareness among the public together with the use of outdated and non-licensed software are the main problems.

Several common challenges hamper the development of cybersecurity resilience in the EaP countries.[11] By and large, the low level of general awareness among the public together with the use of outdated and non-licensed software are the main problems. At the end of the day, the efficacy of the attacks depends foremost on people's behaviour. If, for instance, an individual clicks on an advertisement on social media or in their email containing malware or a link to a phishing site, that may enable penetration by hackers to the user's whole network. On the state level, the most important limiting factors are conflicts over the national authorities' responsibilities, a lack of qualified staff with relevant digital skills and high turnover in the sector, as well as a scarcity of technologies to secure networks. These all stymie effective monitoring and limit the response to cyber incidents. Moreover, cooperation is weak between the state and private sector, which owns and controls critical infrastructure. This also limits the collection of information on cyber incidents. The countries lack a standardised cyberthreat assessment. When it comes to countering cybercrime, in all EaP countries criminal justice systems have scant resources and low capacities to prevent, investigate, prosecute, and adjudicate cybercrime involving electronic evidence.

EU-EaP Countries Cybersecurity Cooperation: State of Play

The EU is interested in collaborating with the EaP region on cyber issues because it impacts the Union's stability. Technologies tested during cyberattacks in Ukraine are being used in Western countries. On the EU side, the scope of cooperation is hampered by its limited competences in the field. It does not have a common cybersecurity threat assessment, lacks the operational capacity to analyse and respond to cross-border cyberattacks, and intelligence sharing between Member States is fragmented. For their part, EaP countries, which have various security situations, differ in terms of their ambition to apply EU solutions and standards. By and large, countries that have signed

10 "Significant Cyber Incidents Since 2006," CSIS database, www.csis-website-prod.s3.amazonaws.com.

11 See studies held in the scope of the CyberEast programme, Council of Europe, www.coe.int.

Association Agreements (AAs) or Comprehensive and Enhanced Partnership Agreement (CEPA),[12] containing provisions on cybersecurity, are calling for deeper integration with the EU in this field. For Georgia and Ukraine, enhanced partnership with NATO, to which most EU Member States belong, facilitate cooperation with the Union in general. Other EaP countries, such as Belarus and Azerbaijan, want to exchange practices to better secure their network systems. A challenge is the participation of Belarus and Armenia in the Eurasian Economic Union (EAEU) and Collective Security Treaty Organisation (CSTO), as these states adopt similar conceptual approaches to information security as Russia (e.g., common model of information security threats and e-signature systems; public authorities use Russian software products).[13]

The EU has not yet clarified its overall conceptual approach to supporting the cyber resilience of EaP countries.

However, the EU has not yet clarified its overall conceptual approach to supporting the cyber resilience of EaP countries. So far, it has been treated as a sub-priority of EU actions, particularly in countering organised crime or as part of the wider EU digital agenda by addressing the civilian aspects of cybersecurity. Regionally, the EU aims primarily to counter cybercrime by convincing EaP countries fulfil the Budapest Convention.[14] This is a legally binding international treaty defining national legislation against cybercrime and international cooperation in this field. At the multilateral level, the EU addresses the prevention of cyberattacks to some extent by helping countries to adapt cyber strategies and strengthen or create Computer Emergency Response Teams (CERTs), units responsible for monitoring cyber incidents and the response. Bilaterally, in the case of AA/CEPA countries, the EU focuses to a greater extent on the protection of critical infrastructure based on the standards of the Network and Information Security (NIS) Directive.[15] The directive obliges the countries to, among others, develop national cyber capabilities and identify and supervise critical infrastructure. To fulfil all those objectives, the EU engages in a political dialogue at the multilateral and bilateral levels, supported by aid.

EaP Multilateral Format

At the regional level, EaP cybersecurity is debated mainly through the Panel on Security, Common Security and Defence Policy and Civil Protection and the Panel on Harmonisation of Digital Markets. Importantly, despite the 2020 escalation between Armenia and Azerbaijan in Nagorno-Karabakh in 2020 and the political crisis in Belarus, experts from those countries participate in discussions on technical matters. The EU has been mainly financing programmes on countering cybercrime led by the Council of Europe (around €7 million in the years 2011-2022). In 2019, it launched the first programme on cyber resilience—EU4Digital Cybersecurity East programme (€3 million) related to the protection of critical infrastructure and countering cyberattacks. So far, the main results of this regional cooperation have been the adoption by all EaP countries of cybercrime strategies and cybercrime units. Most of them (with the exception of Armenia) have created CERTs, but they require further strengthening. Associated countries signed operational agreements with Europol and Eurojust. Still, no EaP country has fully implemented the Budapest Convention.

The EU also has some regional instruments to counter disinformation. The central structure in this respect is Eastern Strategic Communications (East StratCom), a task force consisting of 13 officials and located in the European External Action Service, covering the EaP region. Its work will be

12 Georgia, Moldova, and Ukraine signed an AA; Armenia has signed a CEPA.

13 P. Pernik, "EU's Cyber Capacity Building in the Eastern Partnership Countries," ICDS blog, 13 October 2017, www.icds.ee.

14 "Budapest Convention and related standards," Council of Europe, www.coe.int. Belarus has not acceded to the Convention but has expressed willingness to join.

15 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016, www.eur-lex.europa.eu.

strengthened by new personnel in EU delegations covering strategic communication (one per delegation). East StratCom is responsible for monitoring mainly Russian disinformation, delivering analysis in this field, and raising awareness. It contributes also to the design of EU communication in the EaP region and media literacy programmes. It gives examples of its action via the website EUvsdisinfo.eu and distributes regular newsletters. In Georgia, through East StratCom's budget, it has supported the introduction of fact-checker organisations into international networks to strengthen their voice on social media platforms. Beside this task force, the EU has been supporting independent media in the EaP region for years. Still, regional funding for media is low in comparison to other aid donors. The EU's major six-year EU4IndependentMedia programme, covering all EaP countries, has budget of €11 million, while a recent three-year UK programme in Ukraine was €10 million.[16]

Cybersecurity Cooperation in EU Bilateral Relations with EaP Countries

EU political and financial cooperation on cyber resilience is most advanced with Ukraine and Georgia, but with the other EaP countries it remains limited.

At the bilateral level, EU political and financial cooperation on cyber resilience is most advanced with Ukraine and Georgia, but with the other EaP countries it remains limited. The EU stands politically engaged in the cyber arena with associated countries. It officially condemned the cyberattacks in Georgia (2019) and in Ukraine (2017) and promised to support the countries.[17] Both partners align with EU statements towards third countries in the field of cybersecurity and EU cyber sanctions. A milestone was the Union's decision to launch a cyber dialogue with Ukraine in October 2020. It became the seventh country with which the EU has launched this format (the others are Brazil, China, India, Japan, South Korea, U.S.). A cyber dialogue enables the exchange of information on cyberattacks at a high political level and mobilises various European Commission units to contribute. In the near future, the EU plans, for instance, to launch a programme for Ukraine on cyber diplomacy in international forums (e.g., in the field of cybercrime at the UN level).

Both Ukraine and Georgia recently strengthened some angles of cybersecurity cooperation with the EU. The Georgian and Ukrainian authorities frequently inform the EU about cyberattacks through diplomatic channels, but they might also report on an ad hoc basis at the level of the EU Hybrid Fusion Cell, responsible for Member State intelligence-sharing. Second, the EU Monitoring Mission in Georgia and the EU Advisory Mission in Ukraine have been reinforced by several experts responsible for cyber threats and disinformation. To the latter mission, the EU allocated around €2.5 million to strengthen its cyber capacities. Finally, Georgia and Ukraine can enter some trainings provided by the European Security and Defence College, a major EU centre training Member State officials in the security field. A new programme dedicated to cybersecurity for neighbourhood and Western Balkans countries is planned to launched in the first half of 2021.

In terms of aid, the EU primarily finances advisory services and trainings, helping with legislative and institutional approximation to EU standards through short- and long-term expert missions.[18] A few

16 "UK announces £9 million project to support independent media in Ukraine" (press release), UK Government, 2 July 2019, www.gov.uk.

17 "Declaration by the High Representative on behalf of the European Union—call to promote and conduct responsible behaviour in cyberspace" (press release), 21 February 2020, and

"Council Conclusions on malicious cyber activities," 16 April 2018, Council of the European Union, Brussels, consilium.europa.eu.

18 See the list of EU financed projects at "Cybersecurity guidelines for the Eastern Partnership region," EU4Digital, June 2020, www.eufordigital.eu.

projects involve practical exercises or the delivery of equipment. One project including exercises focused on countering election-related cyber threats and disinformation in Ukraine in 2019.[19] A positive development is the plan to supply equipment to increase Ukraine's cyber resilience under a new EU programme to support e-governance and the digital economy. In terms of aid results, the cooperation is recent so the EU is in the initial phase of helping its partners adapt to its NIS directive standards. So far, it has presented its standards and the partners are assessing their needs to be addressed.

In aid delivery, the European Commission ensures Member State participation in its financed projects. Estonia is the most active in this respect. Other countries, depending on their cyber capacities, take part in some specific projects (e.g., the Baltic States, Poland, Slovakia, the Netherlands, Finland, but also Germany, Austria, and Spain). To illustrate, Poland has advised Ukraine on cybersecurity strategy. Importantly, Ukraine and Georgia cooperate with Member States through NATO. For instance, NATO launched the Ukraine Cyber Defence Trust Fund (2015-2017), led by Romania, which helped with equipping digital labs to investigate cybersecurity incidents. Both countries are also participants or observers in various cyber exercises, such as *Locked Shields*. Last but not least, EU delegations, through regular donor onsite meetings, coordinate Union aid with the UK and U.S. For example, under the Countering Malign Kremlin Influence[20] programme, the U.S. has provided equipment (IT hardware, software, and protocols) to central elections committees in Georgia and Moldova, while its advisors have been training energy company personnel on cybersecurity technologies in Ukraine.

Conclusion and Recommendations

Cyberattacks coupled with online disinformation pose a serious risk to the resilience of EaP countries. While exposure to cyber threats and the level of cyber-security systems varies by EaP country, all of them face numerous institutional, legal, and operational shortcomings in this respect. The EU advances mainly its collaboration with Ukraine and Georgia, but it pursues a common agenda for the whole EaP region. In doing this, the EU focuses on the exchange of experience as well as legal and institutional approximation to its standards, while it largely omits equipping partners with technologies.

Strengthening cybersecurity cooperation would be beneficial for the EU as it could learn from cyberattacks in the region and reflect that experience in its own crisis-response system.

Strengthening cybersecurity cooperation would be beneficial for the EU as it could learn from cyberattacks in the region and reflect that experience in its own crisis-response system. For EaP countries heavily impacted by the economic crisis due to the COVID-19 pandemic, EU-financed capacity-building programmes would be worthwhile. To maximise such collaboration, the EU could undertake the following actions.

The EU could strengthen the political dialogue on cybersecurity with associated countries, which call for deepening collaboration in this field. Like in Ukraine, the EU might launch a cyber dialogue with Georgia and, in the long term, possibly also with Moldova, depending on the developments of the internal political situation there. As part of such political dialogue, AA countries could align with EU positions on cybersecurity in international forums

19 "Project: Countering Election-related Cyber Threats and Disinformation Campaigns in Ukraine, Project description," ECEAP, www.eceap.eu.

20 "Countering malign Kremlin influence. Development Framework. Implementation Report," USAID, 2020, www.usaid.gov.

or follow its 5G Toolbox in practise. Cyber dialogues should aim to facilitate the adoption of action plans, including concrete steps to be achieved to protect critical infrastructure. This should go hand in hand with EU financial assistance for trainings of personnel in specified companies delivered by EU consortia; providing relevant equipment such as information-sharing protocols and mechanisms and software (e.g., through budget support operations whenever possible) and delivery of practical exercises on cyber operations and investigations. The EU missions in Georgia and Ukraine should have a special training programme on cyberthreats and could benefit from short-term Member State expert missions to help with cyber-related tasks.

Irrespective of cyber dialogues, the EU could strengthen operational cooperation with associated countries. First, some of them might join Permanent Structured Cooperation (PESCO) projects related to cybersecurity (e.g., project on cyber rapid-response teams, led by Lithuania), depending on whether their participation adds value to the project. To do so, Member States participating in the project should recommend including third countries and the Council must agree by unanimous vote.

Second, depending on the willingness of the Member States, AA countries might associate with the intergovernmental European Centre of Excellence for Countering Hybrid Threats in Helsinki, which would enable common trainings and workshops. Third, in the longer term, after implementing the basis of the NIS directive, some of them could gain observer status in the European Union Agency for Cybersecurity, allowing them to participate in practical exercises. Last but not least, in associated countries and Armenia, the EU could develop stronger action on the prevention of cyberattacks during periods of national elections. For instance, it might launch mechanisms to support resilient electoral processes and protect election infrastructure against cyberattacks, similar to ones the EU will adopt in 2021.[21]

At the multilateral level in the EaP, the EU should continue the collaboration based on the existing, established priorities. Bearing in mind the limited resources, it should focus only on several areas of countering cybercrime, such as cross-border access to electronic evidence for criminal investigations or prevention of child-related cybercrime. When it comes to cybersecurity incident management, the EU should further work to strengthen CERT operations and support them through regional funding schemes. Moreover, it would be worthwhile to develop a cyberthreat assessment for the region, including analysis of cyber operations, disinformation, and electoral interference, to enable the Member States to better understand the developments in the region. In this respect, the EU could support the development of an internationally recognised index assessing countries' disinformation resilience (to cover at least the EU, Western Balkans, and the Union's eastern and southern neighbourhoods).

The biggest potential is in boosting EU capacities on countering disinformation and strengthening the resilience of societies in this respect. Primarily, the EU should significantly increase financing for local independent media and diversify both the implementing partners and final beneficiaries of its aid. A good example to follow is the current regional programme in Ukraine, which includes media literacy components. The EU might also work out a programme financing education modules for schools on disinformation and critical-thinking for youth based on, for example, the Finnish experience in this field. The EU could further increase the capacities of East StratCom—both in terms of budget and personnel—to enable it to develop proactive actions, for example, supporting the dialogue between fact-checker organisations and social media giants.

21 "Communication on the European democracy action plan," European Commission, 3 December 2020, pp. 6-7.

Table 2. Cybersecurity Indices for EaP Countries

Index	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Global Cybersecurity Index 2018 (193 members)	79	55	69	18	53	54
National cybersecurity Index 2021 (160 assessed countries)	92	77	51	43	54	25

Source: Own compilation, PISM data.