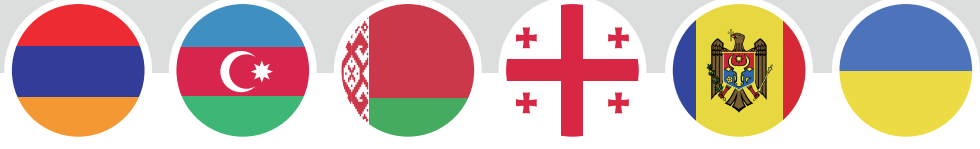
EU2017.EE

EaP Eastern Partnership

eGA e-governance academy 15 YEARS Empowering e-governance around the world

Policy Recommendations on Safety and Security in the Cyberspace and on E-Democracy



ESTONIA DEVELOPMENT COOPERATION

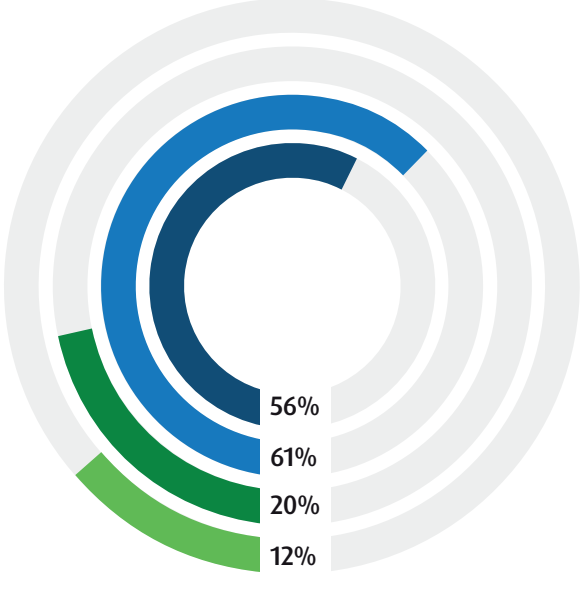
SWEDEN

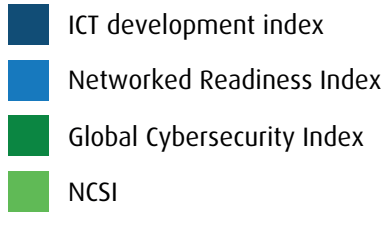
Policy recommendation on safety and security of the cyberspace

Armenia

Regarding the general ICT development, Armenia has fulfilled 56% of the ICT development index (2016). It places Armenia in 71st place in the index. According to the Networked Readiness Index (2017), Armenia has fulfilled 61% of the maximum criteria. It places Armenia in 56th place in the index. Both these indices show that general ICT development in Armenia is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Armenia has fulfilled 20% of the criteria. It places Armenia in 110th place in the world. Our current study (NCSI) shows that Armenia has fulfilled 12% of the cyber security criteria.





In general, it means the gap between ICT development and cyber security is relatively large. Armenia has paid attention to ICT development, but now it also needs to pay attention to cyber security development.

There is good progress in the area of combating cybercrime where Armenia fulfils 60% of the criteria. Armenia has criminalised cybercrimes, and has a unit for digital forensics and 24/7 contact point for international cybercrime.

Additionally, there has been progress in baseline security development and electronic signature areas. Armenia has a personal data protection authority and a legal framework for electronic signature. Such a positive development should be continued.

In general, it seems that Armenia needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

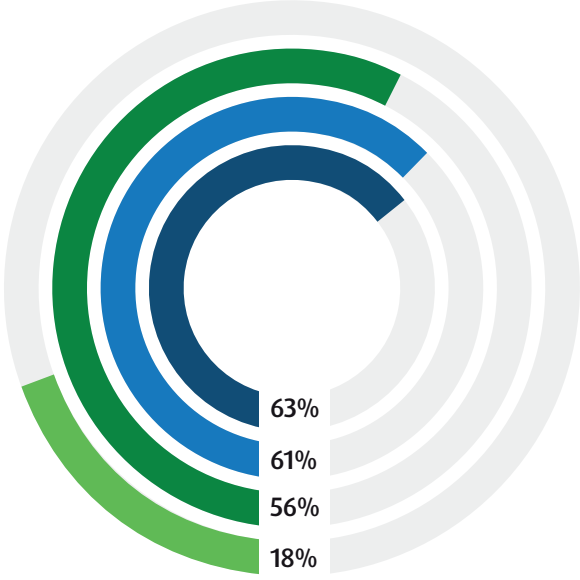
	Percentage of maximum capacity (capacities have different weights)	12.12%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	0%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	0%
4.	International cooperation in the cyber security field	10%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	27%
6.	Secure environment for e-services	0%
7.	Electronic identification and electronic signature	25%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	0%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	60%
12.	National cyber defence capability	0%

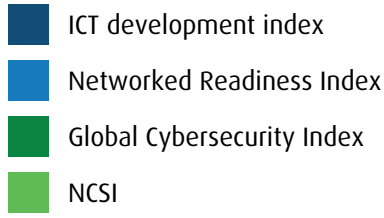
Armenia's cyber security situation according to the NCSI.

Azerbaijan

Regarding the general ICT development, Azerbaijan has fulfilled 63% of the ICT development index (2016). It places Azerbaijan in 58th place in the index. According to the Networked Readiness Index (2017), Azerbaijan has fulfilled 61% of the maximum criteria. It places Azerbaijan in 53rd place in the index. Both these indices show that general ICT development in Azerbaijan is above average.

Regarding the Cyber Security development, the Global Cybersecurity Index (2017) shows that Azerbaijan has fulfilled 56% of the criteria. It places Azerbaijan in 48th place in the world. Our current study (NCSI) shows that Azerbaijan has fulfilled 18% of the cyber security criteria.





In general, it means a gap between ICT development and cyber security exists, and Azerbaijan needs to pay more attention to cyber security development.

There is good progress in the cyber threat analysis area where Azerbaijan has fulfilled 75% of the criteria. Additionally, the electronic identification and electronic signature area is relatively well developed (50%).

From the table, we can also see that there has been some progress in the cyber incident management field (44%), in the international cooperation field (30%), in the cyber security education field (20%), in the field on combating cybercrime (10%) and in the baseline security field (9%).

In general, there are many cyber security areas where Azerbaijan needs to pay attention in order to support good development in the ICT area. It seems that Azerbaijan needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

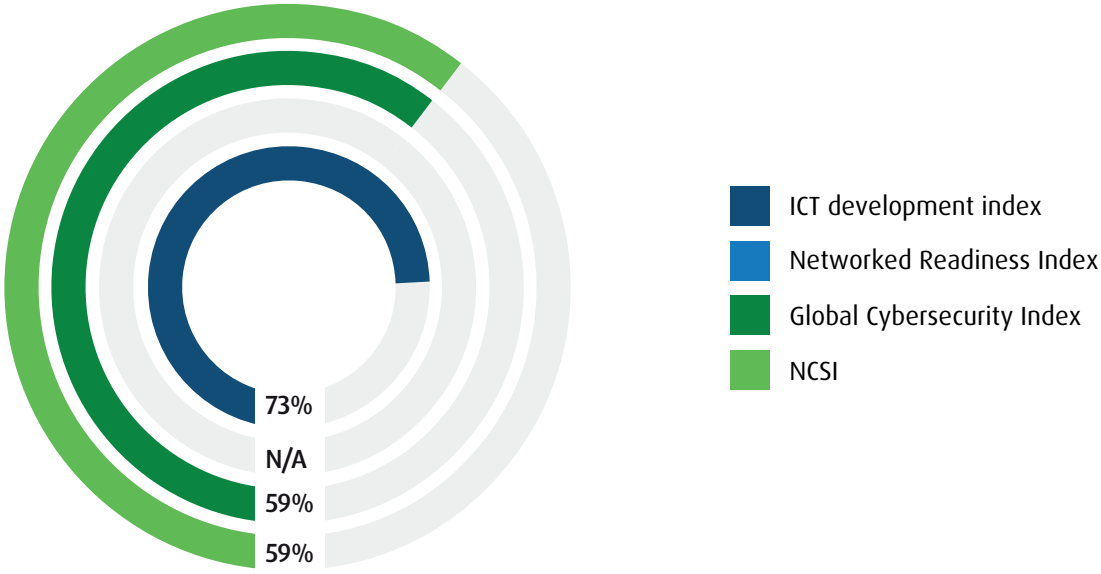
	Percentage of maximum capacity (capacities have different weights)	18.18%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	0%
2.	Understanding and analysis of cyber threats	75%
3.	Cyber security education on all levels and professional development	20%
4.	International cooperation in the cyber security field	30%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	9%
6.	Secure environment for e-services	0%
7.	Electronic identification and electronic signature	50%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	44%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	10%
12.	National cyber defence capability	0%

Azerbaijan's cyber security situation according to the NCSI.

Belarus

Regarding general ICT development, Belarus has fulfilled 73% of the ICT development index (2016). It places Belarus in 31st place in the index. It shows that general ICT development in Belarus is very good.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Belarus has fulfilled 59% of the criteria. It places Belarus in 39th place in the world. Our current study (NCSI) shows that Belarus has also fulfilled 59% of the cyber security criteria.



In general, cyber security development in Belarus is above average (59% of the maximum). However, taking into consideration that ICT development is much higher (73% of the maximum), more attention needs to be paid to cyber security.

There are four areas where Belarus has 100% capacity. These areas are (6.) secure environment for e-services, (7.) electronic identification and electronic signature, (8.) protection of essential e-services and critical information infrastructure and (9.) capacity to manage cyber incidents.

The less developed areas are (10.) management of large-scale cyber crises, (4.) international cooperation in the cyber security field, and (1.) policy development. Belarus has taken part in an international cyber crisis management exercise, but it lacks the national capacity to manage cyber crises. Additionally, in the international cooperation area, Belarus needs progress. For example, Belarus has not implemented the Council of Europe's Convention on Cybercrime.

Regarding the cyber policy development, Belarus has a coordination format, but no specialised unit for policy development. Additionally, Belarus lacks cyber security terms and definitions, national cyber security strategy and a national level implementation plan.

In general, the Belarusian cyber security situation is relatively well developed and this good progress needs to be taken further.

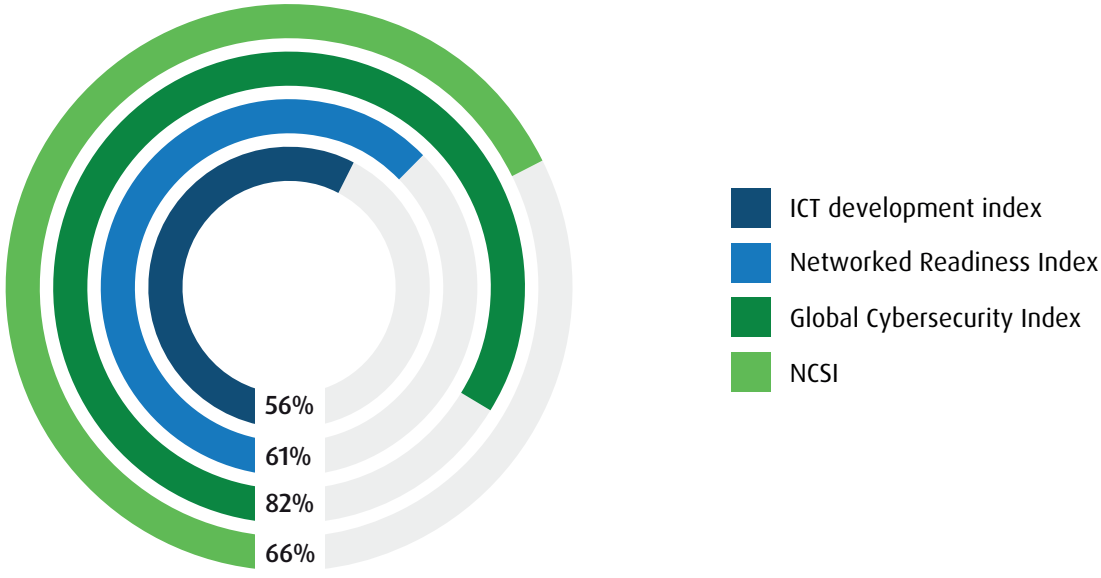
	Percentage of maximum capacity (capacities have different weights)	59.09%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	25%
2.	Understanding and analysis of cyber threats	75%
3.	Cyber security education on all levels and professional development	55%
4.	International cooperation in the cyber security field	20%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	55%
6.	Secure environment for e-services	100%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	100%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	100%
10.	Capacity to manage large-scale cyber crises	11%
11.	Fight against cybercrime	60%
12.	National cyber defence capability	60%

Belarus' cyber security situation according to the NCSI.

Georgia

Regarding general ICT development, Georgia has fulfilled 56% of the ICT development index (2016). It places Georgia in 72nd place in the index. According to the Networked Readiness Index (2017), Georgia has fulfilled 61% of the maximum criteria. It places Georgia in 58th place in the index. Both these indices show that general ICT development in Georgia is above average.

Regarding the Cyber Security development, the Global Cybersecurity Index (2017) show that Georgia has fulfilled 82% of the criteria. It places Georgia in 8th place in the world. Our current study (NCSI) shows that Georgia has fulfilled 66% of the cyber security criteria.



Georgia is one of the few countries where cyber security development is ahead of ICT development. From the cyber security point of view, the situation is very good. Now it is necessary to consider how to balance cyber security development with ICT development.

Georgia has maximum level capacity (100%) in five areas: (1.) policy development, (2.) understanding and analysis of cyber threats, (7.) electronic identification and electronic signature, (8.) protection of essential e-services and critical information infrastructure, and (11.) fight against cybercrime. It is very good that centrally important capacities like policy development and threat analysis have maximum scores. It shows that the potential for balanced security development is high.

Additionally, the (9.) incident management area, (6.) secure environment for e-services, and (5.) baseline cyber security are relatively well developed. Areas that need the most attention are (3.) cyber security education, (12.) cyber defence capability, (4.) international cooperation and influence, and (10.) management of large-scale cyber crises.

In general, we can say the national-level cyber security is very well arranged in Georgia. Despite the fact that there are some areas that need attention, the overall cyber security capacity is well organised in Georgia.

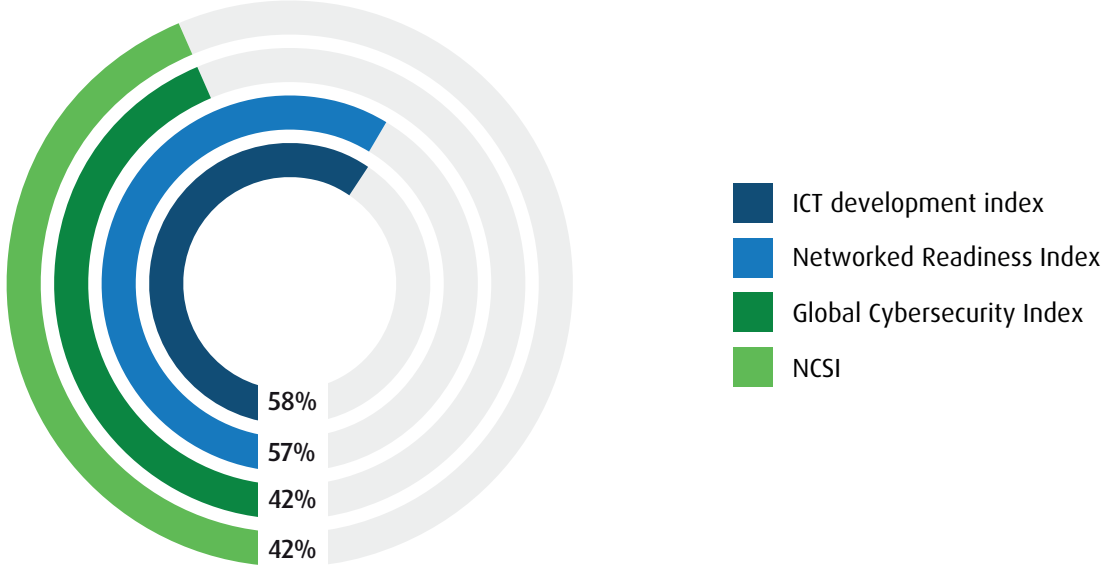
	Percentage of maximum capacity (capacities have different weights)	65.66%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	100%
2.	Understanding and analysis of cyber threats	100%
3.	Cyber security education on all levels and professional development	20%
4.	International cooperation in the cyber security field	40%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	64%
6.	Secure environment for e-services	75%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	100%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	89%
10.	Capacity to manage large-scale cyber crises	33%
11.	Fight against cybercrime	100%
12.	National cyber defence capability	20%

Georgia's cyber security situation according to the NCSI.

Republic of Moldova

Regarding general ICT development, Moldova has fulfilled 58% of the ICT development index (2016). It places Moldova in 68th place in the index. According to the Networked Readiness Index (2017), Moldova has fulfilled 57% of the maximum criteria. It places Moldova in 71st place in the index. Both these indices show that the general ICT development in Moldova is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Moldova has fulfilled 42% of the criteria. It places Moldova in 72nd place in the world. Our current study (NCSI) shows that Moldova has also fulfilled 42% of the cyber security criteria.



Moldova has made significant developments in the areas of (6.) secure environment for e-services, (7.) electronic identification and electronic signature, and (11.) fight against cybercrimes. In all these areas Moldova has got 100% of the maximum level.

Additionally, baseline cyber security is relatively well developed in Moldova (73% of the maximum). Moldova has a personal data protection authority, legislation for information classification, minimum requirements for cyber security, and requirements for ICT systems' audit. An important capability that Moldova doesn't have at the moment is a responsible authority for cyber security. It is a very important capability that needs to be developed in the near future.

Areas where Moldova has made some progress are (1.) policy development, (3.) education, (4.) international cooperation and (9.) cyber incident management. Moldova has a national programme for cyber security development (strategy) and implementation plan. What is needed in the policy development area is clear management and coordination.

Regarding education, Moldova has a cyber safety website and several public awareness activities. Addi-

	Percentage of maximum capacity (capacities have different weights)	42.42%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	38%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	30%
4.	International cooperation in the cyber security field	10%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	73%
6.	Secure environment for e-services	100%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	56%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	100%
12.	National cyber defence capability	0%

Moldova's cyber security situation according to the NCSI.

tionally, Moldova has a cyber security programme on the bachelor's level. In the future, Moldova needs to pay more attention to general cyber safety education in schools as well as professional development.

Regarding incident management, Moldova has a 24/7 Government Computer Incident Response Team. At the same time, Moldova lacks a regulation that makes reporting about cyber incidents compulsory. Additionally, Moldova needs to pay attention to the creation of a format for public-private cooperation.

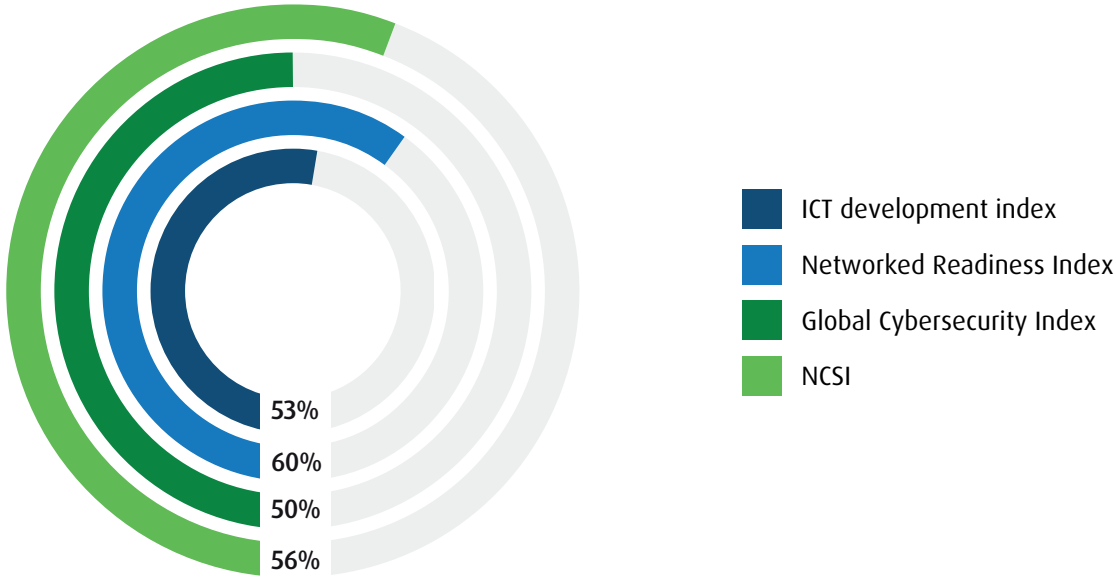
Areas where Moldova needs developments the most are (2.) cyber threat analysis, (8.) protection of essential e-services and critical information infrastructure, (10.) capacity to manage large-scale cyber crises, and (12.) national defence capabilities.

In general, it seems that Moldova needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

Ukraine

Regarding general ICT development, Ukraine has fulfilled 53% of the ICT development index (2016). It places Ukraine in 76th place in the index. According to the Networked Readiness Index (2017), Ukraine has fulfilled 60% of the maximum criteria. It places Ukraine in 64th place in the index. Both these indices show that general ICT development in Ukraine is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Ukraine has fulfilled 50% of the criteria. It places Ukraine in 58th place in the world. Our current study (NCSI) shows that Ukraine has fulfilled 56% of the cyber security criteria.



In general, ICT development and cyber security development in Ukraine are about the same level. From the cyber security perspective, the balance between these areas is good. It should be kept in mind during the information society development.

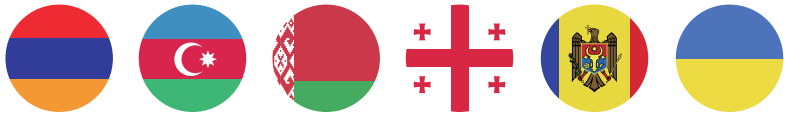
There are five cyber security capacities that are very well developed in Ukraine. These are (11.) fight against cybercrime, (1.) policy development, (5.) baseline cyber security, (7.) electronic identification and electronic signature, and (3.) cyber security education. In these areas, Ukraine has got 75–90% of the maximum capacity.

The less developed areas are (2.) understanding and analysis of cyber threats, (12.) national cyber defence capability, (4.) international cooperation, (6.) secure environment for e-services and (10.) capacity to manage large-scale cyber crises.

There are many areas where Ukraine needs specific and sectorial cyber security capacity development. Cyber threat analysis and information dissemination among the general public, businesses and the public sector are certainly capacities that need to be taken in focus. It will make society stronger and better prepared for cyber incidents. National cyber defence capacity is another area where significant developments are needed.

	Percentage of maximum capacity (capacities have different weights)	56.06%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	88%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	75%
4.	International cooperation in the cyber security field	20%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	82%
6.	Secure environment for e-services	25%
7.	Electronic identification and electronic signature	88%
8.	Protection of essential e-services and critical information infrastructure	67%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	67%
10.	Capacity to manage large-scale cyber crises	33%
11.	Fight against cybercrime	90%
12.	National cyber defence capability	0%

Ukraine's cyber security situation according to the NCSI.



General recommendations on safety and security of the cyberspace

As a general principle, national cyber security capacity development has to be approximately on the same level as ICT development in the country. If a country is interested in information society development, the country has to pay equal attention to cyber security.

These areas must be balanced. The following table gives a general overview about EaP countries' ICT development and cyber security development and shows the gap between these areas.

General overview regarding EaP countries' ICT and Cyber Security Development.

% of the maximum level	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ICT development	58.5%	62%	73%	58.5%	57.5%	56.5%
ICT Development Index	56%	63%	73%	56%	58%	53%
Networked Readiness Index	61%	61%	N/A	61%	57%	60%
Cyber security development	16%	37%	59%	74%	42%	53%
Global Cybersecurity Index	20%	56%	59%	82%	42%	50%
Current Study (NCSI)	12%	18%	59%	66%	42%	56%
Gap						
Gap	42.5	25	14	15.5	15.5	3.5

According to the table, the most balanced situation is in **Ukraine**. The average ICT development percentage is 56.5 and the cyber security average development is 53%. The gap is only 3.5 percentage points.

Georgia is the only country where cyber security development is ahead of ICT development. The ICT development average is 58.5% and the average cyber security development is 74%. The gap is 15.5 percentage points and it favours cyber security.

The following table gives general results of the current study. The dark green colour shows capacities that are completed 50% or more. The light green colour shows capacities that are completed 25-50%. The white colour shows capacities that are completed less than 25%.

General overview of countries' results.

		Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
I	GENERAL CYBER SECURITY INDICATORS						
1.	Policy development	0%	0%	25%	100%	38%	88%
2.	Threat assessment	0%	75%	75%	100%	0%	0%
3.	Education	0%	20%	55%	20%	30%	75%
4.	International cooperation	10%	30%	20%	40%	10%	20%
II	BASELINE CYBER SECURITY INDICATORS						
5.	Baseline security	27%	9%	55%	64%	73%	82%
6.	E-services security	0%	0%	100%	75%	100%	25%
7.	E-ID and e-signature	25%	50%	100%	100%	100%	88%
8.	CIIP	0%	0%	100%	100%	0%	67%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS						
9.	CIRC	0%	44%	100%	89%	56%	67%
10.	Crisis management	0%	0%	11%	33%	0%	33%
11.	Cybercrimes	60%	10%	60%	100%	100%	90%
12.	National defence	0%	0%	60%	20%	0%	0%

The table indicates areas where EaP countries are doing well and areas that need more attention. We recommend prioritising cooperation areas where EaP countries have common cyber security shortcomings.

According to the results, we can say that the best developed capacities are:

- Baseline security
- E-ID and E-signature
- Computer Incident Response Capacity
- Fight against cybercrime

The less developed areas are:

- International cyber security development and influence
- Cyber crisis management
- National defence capability in the cyber field

More specifically, an overview of EaP countries' cyber security situation is presented in the following table. It gives an overview on YES (x) and NO (-) basis and indicates what specific capacities exist in the countries and what capacities need to be developed.

For example, one of the areas where all EaP countries need capacity-building is cyber security knowledge in primary education. There is a need to teach basic online and computer security aspects to children. Additionally, the table indicates that a professional association for cyber / information security experts exists only in Ukraine. Other EaP countries lack this capacity.

Another area where all EaP countries need capacity development is Cyber Crisis Management. None of the EaP countries have a crisis management plan for large-scale cyber incidents. A Cyber Operations Centre exists only in Ukraine. Cyber crisis management exercises are organised only in Belarus. A couple of countries have taken part in international cyber crisis management exercises. All these aspects indicate that cyber crisis management capacity development should be in focus.

Detailed overview of countries' results.

		Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
I	GENERAL CYBER SECURITY INDICATORS						
1.	Policy development	0%	0%	25%	100%	38%	88%
	Policy development unit	-	-	-	X	-	X
	Coordination format	-	-	X	X	-	X
	Terms and definitions	-	-	-	X	X	-
	Cyber security strategy	-	-	-	X	X	X
	Implementation plan	-	-	-	X	X	X
2.	Threat assessment	0%	75%	75%	100%	0%	0%
	Threat analysis unit	-	X	X	X	-	-
	Annual public reports	-	-	-	X	-	-

3.	Education	0%	20%	55%	20%	30%	75%
	Cyber safety website	-	X	-	X	X	X
	Public awareness-raising	-	X	-	X	X	-
	Primary education	-	-	-	-	-	-
	Secondary education	-	-	X	-	-	-
	Vocational education	-	-	X	-	-	-
	Bachelor education	-	-	X	-	X	X
	Master's education	-	-	X	-	-	X
	PhD education	-	-	X	-	-	X
	Professional association	-	-	-	-	-	X
4.	International cooperation	10%	30%	20%	40%	10%	20%
	Cooperation unit	-	-	-	-	-	-
	Convention on Cybercrime	X	X	-	X	X	X
	Cooperation agreement	-	X	X	X	-	-
	Internat. representation	-	X	X	X	-	X
	Int. Org. in the country	-	-	-	-	-	-
	Capacity-building	-	-	-	X	-	-
II	BASELINE CYBER SECURITY INDICATORS						
5.	Baseline security	27%	9%	55%	64%	73%	82%
	Baseline security unit	-	-	X	X	-	X
	Data protection authority	X	-	-	X	X	X
	Information classification	-	X	X	X	X	X
	Security standard	-	-	-	-	X	-

	ICT systems' accreditation	-	-	X	-	X	X
	ICT systems' audit	-	-	X	-	X	X
6.	E-services security	0%	0%	100%	75%	100%	25%
	E-services security	-	-	X	X	X	-
	Up-to-date cryptography	-	-	X	-	X	X
7.	E-ID and e-signature	25%	50%	100%	100%	100%	88%
	Unique identifier	-	-	X	X	X	X
	E-services use unique ID	-	-	X	X	X	X
	2-factor authentication	-	X	X	X	X	-
	Electronic signature	X	X	X	X	X	X
	Trust services providers	-	X	X	X	X	X
	E-signature is legal	X	X	X	X	X	X
8.	CIIP	0%	0%	100%	100%	0%	67%
	CII is defined	-	-	X	X	-	X
	Protection unit	-	-	X	X	-	X
	Continuity requirements	-	-	X	X	-	-
	Cyber security manager	-	-	X	X	-	-
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS						
9.	CIRC	0%	44%	100%	89%	56%	67%
	CIRC unit	-	X	X	X	X	X
	Reporting responsibility	-	-	X	-	-	X
	Public-private cooperation	-	-	X	X	-	-
	Exchange classified info	-	-	X	X	X	X

10.	Crisis management	0%	0%	11%	33%	0%	33%
	Crisis management plan	-	-	-	-	-	-
	Operations centre	-	-	-	-	-	X
	Exercise with cyber comp.	-	-	-	-	-	-
	Cyber crisis exercise	-	-	-	X	-	-
	Participation in Int. Ex.	-	-	X	X	-	-
	Usage of volunteers	-	-	-	-	-	-
11.	Cybercrimes	60%	10%	60%	100%	100%	90%
	Criminalisation	X	-	X	X	X	X
	Unit for cybercrimes	-	-	X	X	X	X
	Unit for digital forensics	X	-	-	X	X	X
	Evidence is regulated	-	-	-	X	X	-
	24/7 contact point	X	X	X	X	X	X
12.	National defence	0%	0%	60%	20%	0%	0%
	Cyber Ops planning unit	-	-	-	-	-	-
	Cyber operation unit	-	-	X	-	-	-
	Exercise with cyber comp.	-	-	-	X	-	-
	Cyber Ops exercise	-	-	X	-	-	-
	Participation in Int. Ex.	-	-	X	X	-	-

Policy recommendation on e-democracy

Armenia

- The experience of Armenia in **governance innovation** (via pop-up innovation lab) should be promoted and encouraged further. The openness and the willingness of the main governmental actors in the field cannot be overestimated.

- Armenia has a variety of e-solutions; however, with rather low usability. **A lot still has to be done in the public awareness domain.** All stakeholders are encouraged to work on the elaboration of a thorough and comprehensive overview of the e-democracy tools created in order to build a "menu" of different tools that both civil society and government could use.

- The area of **open data** requires more in-depth understanding by all sectors of society. The **capacity of institutionalised civil society** to use the potential of technologies as well as existing open data in a transformative way should be addressed. The IT community has to be stimulated to be part of the social innovation developments.

- Since the realm of open data and transparency that it enables is becoming more and more widespread, a lot of attention has to be paid to **data protection regulations**, which is an issue of concern according to the study.

- The **local level** in Armenia has active developments supported by NGOs and donors. It is important to continue working in this direction and to raise the awareness of local communities about alternative forms of engagement.

- It is vital to encourage the adaptation and adjustment of new solutions to local needs. There should be **a pragmatic tandem between the donor and the government** enabling piloting of new projects before attempting large-scale implementation. The engagement of the IT community in these pilots (and finding proper stimuli for that) would facilitate synergy between the non-governmental and IT sectors.

Azerbaijan

- **A legal and institutional mechanism and regulation for e-participation is important.** Currently there are no strategies or action plans designed for civic participation or e-participation. The only strategic document that can be considered the government's commitment in terms of transparency and civic participation is the latest OGP Action Plan for 2016–2018. However, as the current status of Azerbaijan in OGP is inactive, its implementation at the moment is hard to predict.

- **Support for monitoring of public information provision is recommended.** Enforcement of the Law on Access to Information, which was adopted in 2005, could be monitored by an institution of Ombudsman of Information, which was initially considered as a necessary body, but was eliminated later on.

- Regarding the online provision of information, **support for local governments in the area of provision of information via official webpages is suggested**. For instance, the development of a template with a specific layout of public information on the webpages of local government. This would facilitate easier access to information on the local level for the residents as well as provide local governments with a fairly easy tool for structuring their information.

- Emphasis should be put on more **homogenous development of e-services**. Currently the accessibility and quality of e-services is still uneven. There are clear forerunners among state authorities, but there are also those who are lagging behind. Yet, it is clear that transformation from offline service delivery to online services requires a supportive legal and institutional mechanism as well as re-design of processes.

- **A monitoring mechanism is needed on the usability and access to e-services** in order to enable citizens to use the full potential of e-services that already exist as well as to design new ones. Additionally, analysis of the monitoring results and the outcomes of this process should be clear. The ASAN Index developed by the Agency also contains monitoring questions, which cover such components as e-information and e-consultation, yet, it is not so clear how the monitoring results and the outcomes of this process are used for developing e-services and e-participation.

Belarus

- There is a need for amendments or renewal of the legislative framework on **the access to public information and data protection** that would take into account developments in the field of ICTs.

- NGOs should more intensively use new mass media in order to promote the topic to the wider audience. It is also essential to raise their awareness about the concept of e-participation in order to facilitate the overall development of participatory culture in the third sector.

- The low level of collaboration between actors and low awareness of each other might impose an obstacle in reaching a bigger impact. It is hence recommended to **enhance networking activities** and engage the Belarusian **analytical community** (e.g. experts, researchers, think tanks) in advocacy campaigns. The donor community, international organisations and development agencies are encouraged to initiate **joint thematic activities for experience sharing and networking.**

- **The local level initiatives** might be the best way to approach the advancement of e-democracy in Belarus. The potential for further developments could be feasible via e-consultation activities about tangible issues, such as city spatial planning.

Georgia

- The predominance of e-democracy instruments focusing on transparency and accountability is observable. Hence, more e-democracy tools focusing **on participation of citizens in the decision-making processes** is needed. The e-petitions platform (ichange.gov.ge) that is now back on the governmental agenda has the potential to drive the area of e-democracy forward. Given the low digital literacy rate, it is recommended to lower the threshold of signatures for a petition in order to not demotivate citizens to use the platform.

- There is a clear need for a modern standalone act of freedom for information, hence the development of **the Freedom of Information Law** addressing among others the topic of disclosure of public sector data remains important. Additionally, establishment of an oversight authority that would monitor and ensure the enforcement of the corresponding legal provisions is recommended.

- **Institutionalised civil society** should be more active in disseminating **their messages** through attractive communication channels. Using social media more intensively for disseminating the results of good governance projects is advisable. Raising public awareness about and proper education on the usage of existing e-democracy instruments elaborated by NGOs should be one of the focal points in development of this area.

- **Targeted training in the governmental sector** (both on local and national levels) on the topic of using ICTs for the enhancement of democratic processes is essential. Deepening the knowledge of public servants on the legal framework regulating transparency in decision-making; on the concepts of e-participation, open data and transparency; as well as building awareness about different e-consultation and e-participation platforms and mechanisms available for different stages of decision-making processes.

Republic of Moldova

- **Coordination mechanisms and distribution of responsibilities** between actors in the field need to be revised in order **to set clear strategical goals and guidelines** for state institutions for their service provision as well as for engagement practices. The area of e-democracy in Moldova has so far been under the responsibility of the e-Government Centre. It will be shifted in the nearest future under the jurisdiction of the State Chancellery. **Collaboration between the e-Government Centre and the State Chancellery** would then be of the utmost importance as well as the proactive work of the latter in building public awareness of existing e-democracy developments. In order to have sustainability of the results achieved by e-Government Centre, **stable funding** from the state budget for this institution has to be ensured.

- Activities of the e-Government Centre that **focus on gathering feedback from citizens** need further support and encouragement. More specifically, these include such undertakings as annual public perception surveys that provide valuable input from year-to-year on what citizens actually want (e.g. services prioritisation, trust in virtual space, etc.)

- To improve the **quality of civic education** it is important to **set up a clear cooperation mechanism for different ministries** coordinating these fields. One important aspect of civic education is the perception of corruption and manipulation with power. Thus, it is important to raise awareness on why to keep track of corruption and how it functions.

- **E-transformation** cannot happen overnight. It requires **good communication management to explain to citizens what the benefits of e-government are**, in particular in the realm of opening up data. Additionally, the mistrust of citizens towards government needs clear addressing, cultural changes might be pushed forward by awareness conducting campaigns. As part of this topic, the question of **privacy protection versus transparency** needs clearer addressing.

- **There should be more emphasis on creating demand and developing skills for using the data.** The e-Government Centre is involved in an **open data** project with donors' funding that enables numerous datasets to be opened. However, better understanding and awareness is needed on what one could do with the data. Additionally, there is a need for more intensive commitment from local governments, since a lot of data that could be potentially interesting for the citizens is local.

- **Collaboration mechanisms between the government and CSOs have to be reinvented/improved.** The National Participation Council has been established as the main platform for this purpose, but there are some changes expected in its operation. Currently it is not seen as an effective communication channel between different stakeholders.

Ukraine

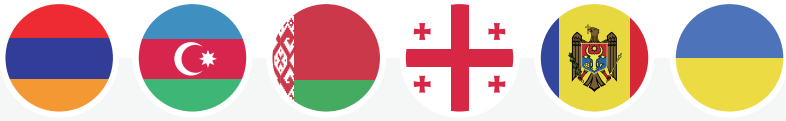
- In the governmental sector, the **institutionalisation of e-democracy** has to take place, i.e. the creation of relevant departments and the allocation of human and financial resources for them. The State Agency is currently taking the coordinating role in this area; however, other governmental institutions also have to become involved. There have to be **clear guidelines** for every institution taking part in the implementation of e-democracy initiatives. Communication departments could be the focal points for e-democracy activities and instruments.

- The massive energy of the Maidan revolution resulted in institutional and instrumental fragmentation in the field of e-democracy, the traces of which can still be visible. **The holistic governmental approach in the area of e-democracy** is now gradually being developed through the development of the E-democracy Concept Paper. This direction and single vision should be encouraged further.

- **The active civil society** of Ukraine should continue performing its proactive role in the development of e-democracy.

- All e-democracy initiatives have to be accompanied by **awareness raising campaigns and training.** A good example of how this kind of awareness raising and training helps to establish a good ecosystem for an e-initiative and make it sustainable is the case of ProZorro.

- Increasing public awareness through **concrete community projects** where different stakeholders are working towards a common agenda could enhance the creation of **a culture of dialogue** and hence, could help Ukrainian e-democracy to flourish.



General recommendations on e-democracy

In view of the above, we would like to draw several general recommendations that we believe could be useful for all countries in the region to take into account:

- All stakeholders should remember that ICTs are instruments at the service of democratic processes. They are the tools that enable societies to advance and "deepen" democracy. Hence, "offline" activities should not be neglected. It is **the combination of online and offline tools** that contributes to the emergence of successful participatory practices.

- All stakeholders are encouraged to cooperate in the work on the elaboration of a thorough and comprehensive overview of available e-democracy instruments in order **to build a "menu" of different tools** that both civil society and government could be using.

- **Local level activism** should be encouraged and nurtured. It plays an essential role in boosting general e-activism in society, being the closest link between citizens and the state.

- **Public awareness and e-literacy campaigns** should be conducted in order to tackle the low usage of e-democracy instruments. Additionally, strong brands around e-democracy tools demonstrating its benefits should be created.

- Targeted training in **the governmental sector** in terms of using ICTs for enhancement of democratic processes is essential. Governments should also acknowledge e-democracy as an integral part of e-governance and underpin its developments with clear strategic and legislative frameworks.

E-democracy is not linked so much to technologies as to the political and cultural choices of every country in terms of the level of involvement of the citizens in the political spheres, the level of accountability and openness.