

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe



Cybersecurity EAST

TERMS OF REFERENCE RESEARCH METHODOLOGY

Activity Code 1.1.2/2.5.3/2.4.1 / PMM 97835

**2088_88 Regional public opinion surveys on cybercrime
reporting and online security**

**Eastern Partnership
May-December 2021**

**Organized by the projects CyberEast, funded by the European
Union and the Council of Europe,
and CybersecurityEast, funded by the European Union**

TABLE OF CONTENTS

1. INTRODUCTION

1.1. Expected Outcome

2. RESEARCH FRAMEWORK

2.1. Research Methodology

2.2. QUANTITATIVE RESEARCH

2.2.1. Sampling Design

2.2.2. Structured by Country (if per-country approach is used)

2.2.2.1. Armenia

2.2.2.2. Azerbaijan

2.2.2.3. Georgia

2.2.2.4. Moldova

2.2.2.5. Ukraine

2.3. QUALITATIVE RESEARCH

3. ANNEXES

Annex 1 – Socio-Demographic Breakdown

Annex 2 – Internet and Social Media Usage

Annex 3 – Country Profiles

Annex 4 – EaP comparative profiles

Annex 5 – Country Cyber State of Play

Annex 6 – Survey: Questionnaire for Individuals

Annex 7 – Survey: Questionnaire for Enterprises

Annex 8 – General Population Focus Group Interview Guide

Annex 9 – Cybercrime Victims Focus Group Interview Guide

Annex 10 – IT Professionals Focus Group Interview Guide

Annex 11 – ISP Professionals Focus Group Interview Guide

Annex 12 – Law Enforcement Focus Group Interview Guide

1. INTRODUCTION

In the world of today, the increasing number of attacks against or realized through the means of computer systems is a growing concern for both cybersecurity professionals and law enforcement, affecting societies at large.

The growing threat of cybercrime seems to be further exacerbated by the COVID-19 pandemic and a massive migration of both work environments and social interaction to online. Thus, the landscape of cybercrime and cybersecurity threats is quickly changing and adapting to the new reality, introducing new threats and challenges for the governmental areas, the private sector and the general public.

Despite growing awareness, the complete picture as to the reporting of cybercrime and cybersecurity incidents, as well as the overall feeling of security in cyberspace for the general public, so far remains unexplored in the Eastern Partnership region (EaP). Moreover, cybercrime and cybersecurity laws and policies developed and adopted by the governments in the region rely on data and input from mostly law enforcement and government security sources, while the perception from the larger population on these threats and challenges is usually not addressed or is used in very limited manner. An example of this were a series of workshops under the former [Cybercrime@EaP 2018](#) project in all Eastern Partnership countries in 2018 as to map threats and challenges with national partners, resulting in a regional Report on the [Perception of threats and challenges of cybercrime in the Eastern Partnership](#); however, findings in the report and stemming from collected data were used only on a few occasions to contribute to strategy/action plan development process in the countries.

In this context, both the [CyberEast](#) project, funded by the European Union and the Council of Europe, and the [CybersecurityEast](#) project, funded by the European Union, aim to support the countries of the Eastern Partnership in improving both their cybersecurity stance and cybercrime-related capabilities of the criminal justice and security community. The focus on needs and concerns of the general public as beneficiaries of the action under these initiatives should therefore be strengthened as to address – primarily, but not exclusively – the matters of the societal perception of threats and challenges originating in cybercrime and cybersecurity, to measure the real use of cybercrime/cybersecurity incident reporting systems, and to assess the ways in which the general public perceives both the security and criminal justice policies of their governments in relation to cyberspace.

Objective and verifiable data collected through surveys would be also a source for additional information as a companion to the [Europol IOCTA report](#), focusing on the Eastern Partnership region countries, further shaping capacity building activities with a focus on the region in the near and mid-term.

1.1. Expected Outcome

Organized by the joint European Union and Council of Europe CyberEast Project – in cooperation with the CybersecurityEast project funded by the European Union – the surveys and overall research effort in the Eastern Partnership region primarily contribute to Output 1.1 of the CyberEast project¹ as well as they simultaneously impact on Outputs 2.4² and 2.5³ through the further assessment of reporting mechanisms.

Results of the surveys will be shared only with the respective countries (regional publication will be discussed separately) and are meant to be used to further contribute to other reporting efforts (e.g.

¹ Output 1.1: National action plans or similar strategic documents regarding criminal justice response to cybercrime and electronic evidence developed.

² Output 2.4: Improved public communication and transparency on cybercrime action

³ Output 2.5: Reinforcing mechanisms for trusted cooperation.

IOCTA) as well as for shaping future policies, strategies and capacity building responses on cybercrime, cybersecurity and electronic evidence in the near and mid-term.

2. RESEARCH FRAMEWORK

The study uniquely tailors both quantitative and qualitative research methods aiming to get a richer and more comprehensive understanding of cybercrime and cybersecurity incidents as perceived by the general public. **The research data should be obtained through face-to-face encounters as much as possible. Whenever this is not possible, then the usage of online means can be employed.**

The research will provide first-hand information about the perception of the citizens towards security in cyberspace, an issue getting immense attention during the COVID-19 pandemic following the increased activity online. Furthermore, the research aims at understanding the institutional capacities to address the issues of concern and mapping those challenges to facilitate the creation of tailor-made policies as well as to strengthening the capacity and policies of the institutions to respond to the citizens' concerns.

2.1. Research Methodology

A combination of quantitative and qualitative research methods will be used to get a better understanding of citizens' perceptions and institutional capacities to respond to challenges and threats.

The data collection process will be carried out across the following CyberEast countries: Azerbaijan, Armenia, Georgia, Moldova and Ukraine. The collection of data will be conducted in September and October 2021 using the same research instruments in each instance (see Annexes), adding country-specific questions tailored to fit the needs and specificities of each EaP country serviced.

2.2. QUANTITATIVE RESEARCH

The data will be collected through face-to-face interviews (as much as possible, if not the usage of online means can be employed) using the **stratified random sampling method** and two unified structured **questionnaires** for the five EaP countries serviced in this project.

Quantitative research questions:

1. What is the attitude of individuals regarding cybercrimes and cybersecurity topics?
2. What is the attitude of enterprises regarding cybercrimes and cybersecurity topics?
3. What are the main concerns and expectations of individuals regarding cybercrime and cybersecurity?
4. What are the main concerns and expectations of enterprises regarding cybercrime and cybersecurity?
5. What are the main differences between individuals and enterprises regarding cybercrime and cybersecurity?

Two main target groups will be followed:

1. Individuals
2. Enterprises

Each target group is approached with tailor-made **questionnaires**. Thus, two questionnaires have been designed for the purpose of this study.

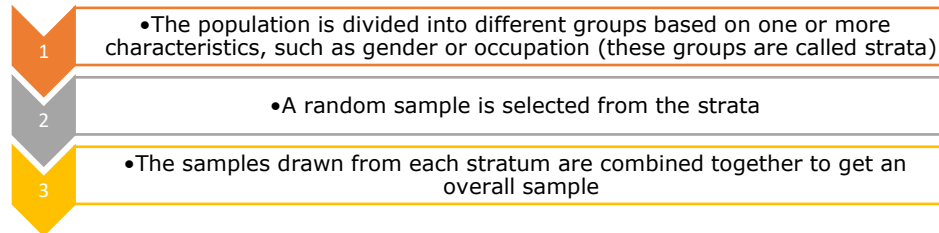
2.2.1. Sampling Design

The data collection method proposed of this scale and nature is the **stratified random sampling** which involves a process of dividing the population into homogeneous subgroups and then extracting a random sample in each subgroup. Therefore, before sampling, members of a population are grouped so that

they form a homogenous subgroup. Stratified sampling ensures that the overall population, including the key subgroups and small minority groups, is represented in the sample.

With regard to the proposed target groups (Individuals and Enterprises), stratified random sampling in each country serviced should follow these three stages:

Graph 1. Three stages of stratified random sampling



The process consists of two-stages sample design, with:

- **Settlements** as **Primary Sampling Units (PSUs)** and
- **Individuals** as **secondary units**

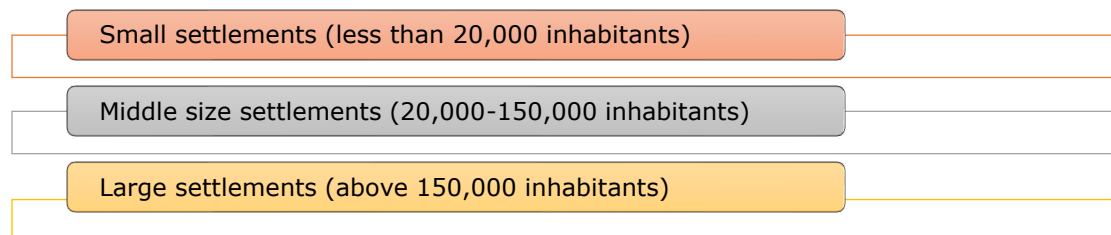
In order to obtain the same structured analysis of the population, the sample first needs to be stratified according to the region or county (depending on the country). At the beginning of the sampling procedure, the number of persons to be interviewed in each region should be defined according to the latest census data and the share of the region in the total population.

The number of respondents should be calculated proportionally to reflect the number of inhabitants in each size of settlements in the region, while the number of sampling points should be defined based on the obtained number of respondents (for each region and in each size of settlement).

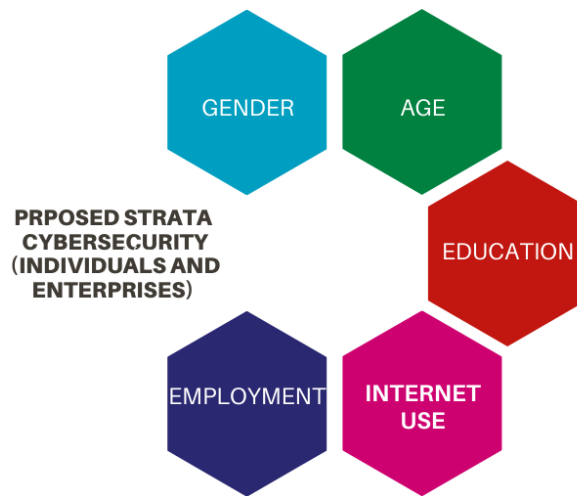
For instance, in the case of the EaP, the sample can be composed of units (cities/towns) and stratified by unit size, expressed in terms of population, level of urbanization and geographical area.

Three settlement classes can be created based on the size of the population/number of inhabitants.

Graph 2. Settlements based on the number of inhabitants



Graph 3. Defining survey strata



In each settlement a total of five (or more) strata can be created to ensure inclusion of all citizens in the survey. Within each stratum, three or four sample units should be randomly selected, with the probability of their selection proportional to their size.

A compromise between an equal allocation and a proportional allocation can be applied in order to ensure distribution in the secondary sampling units (1,000 individuals) by strata. In each selected settlement, a minimum of 20 surveys are to be carried out. Should additional interviews get carried out, the interviews can be distributed proportionally to the PSU's size.

The second-stage sample should also be stratified. In this case, gender, age, education, etc. can be considered for a total of five strata (or more).

After defining the number, the sampling points should be selected randomly, with a probability proportional to the size within each stratum, and according to the latest available census data.

Individuals in each sampling point should be chosen by a random walk method/principle. In a selected individual, the respondent is to be the person whose birthday came latest using the nearest 'birthday method'. Random stratified sampling ensures that each resident in the EaP countries serviced has an equal probability of being chosen for an interview. With the sample used for this study, the results of the survey will mirror trends in attitudes and perceptions amongst the entire adult population (at least 18 years old) of each targeted country in general.

2.2.2. Structured by Country (if a per-country approach is used)

2.2.2.1. Armenia

Data to be collected throughout Armenia through **face-to-face interviews** (or phone, depending on the circumstances created by COVID-19 pandemic) in respondents' homes. The survey should either be face-to-face interviews or by phone, it is not recommended to combine the two approaches.

The representative sample size for Armenia consists of **1,200 permanent residents** aged 18 or older and eligible to vote. It should be representative of the general population by age, gender, region, settlement size and other strata listed above.

Sampling frame: Statistical Committee of the Republic of Armenia latest census grouped in 11 regional groups, age, and gender.

A two-stage probability sampling method is to be used, with random route (walk) and next birthday respondent selection procedures.

- Stage one: All districts of Armenia to be grouped into 11 regions.
- Stage two: The territory of each region to be split into settlements and grouped according to subtype.

Settlements to be selected at random across all regions.

The number of settlements selected in each region to be proportional to the share of population living in the particular type of settlement in each region.

The margin of error should not exceed plus or minus **2.5 percent (maximum level)** for the full sample.

2.2.2.2. Azerbaijan

Data to be collected throughout Azerbaijan between through **face-to-face interviews** (or phone, depending on the circumstances created by COVID-19 pandemic) in respondents' homes. The survey should either be face-to-face interviews or by phone, it is not recommended to combine the two approaches.

The representative sample size for Azerbaijan consists of **1,600 permanent residents** aged 18 or older and eligible to vote. It should be representative of the general population by age, gender, region, settlement size and other strata listed above.

Sampling frame: The State Statistical Committee of the Republic of Azerbaijan latest census grouped in 10 economic regions, age and gender.

A two-stage probability sampling method is to be used, with random route (walk) and next birthday respondent selection procedures.

- Stage one: All districts of Azerbaijan to be grouped into 10 regions.
- Stage two: The territory of each region to be split into settlements and grouped according to subtype.

Settlements to be selected at random across all regions.

The number of settlements selected in each region to be proportional to the share of population living in the particular type of settlement in each region.

The margin of error should not exceed plus or minus **2.5 percent (maximum level)** for the full sample.

2.2.2.3. Georgia

Data to be collected throughout Georgia through **face-to-face interviews** (or phone, depending on the circumstances created by COVID-19 pandemic) in respondents' homes. The survey should either be face-to-face interviews or by phone, it is not recommended to combine the two approaches.

The national sample of Georgia consists of **1,500 permanent residents** aged 18 or older and eligible to vote. It should be representative of the general population by age, gender, region, settlement size and other strata listed above.

A two-stage probability sampling method is to be used, with random route (walk) and next birthday respondent selection procedures.

Sampling frame: National Statistics Office of Georgia.

- Stage one: All districts of Georgia to be grouped into 10 regions.
- Stage two: Selection of the settlements – cities and villages.

Settlements to be selected at random across all regions.

The number of selected settlements in each region to be proportional to the share of population living in a particular type of the settlement in each region.

The margin of error should not exceed plus or minus **2.5 percent (maximum level)** for the full sample.

2.2.2.4. Moldova

Data to be collected throughout Moldova between through **face-to-face interviews** (or phone, depending on the circumstances created by COVID-19 pandemic) in respondents' homes. The survey should either be face-to-face interviews or by phone, it is not recommended to combine the two approaches.

The national sample of Moldova consists of **1,204 permanent residents** of Moldova aged 18 or older and eligible to vote. It should be representative of the general population by age, gender, region, settlement size and other strata listed above.

Sampling frame: Moldova Statistical Databank and by the National Bureau of Statistics.

A two-stage probability sampling method is to be used, with random route (walk) and next birthday respondent selection procedures.

- Stage one: All districts/regions of Moldova to be grouped into 11 groups; all regions
- Stage two: Selection of the settlements (cities and villages).

Settlements to be selected at random across all regions.

The number of settlements selected in each region to be proportional to the share of population living in the particular type of settlement in each region.

The margin of error should not exceed plus or minus **2.5 percent (maximum level)** for the full sample.

2.2.2.5. Ukraine

Data to be collected throughout Ukraine through **face-to-face interviews** (or phone, depending on the circumstances created by COVID-19 pandemic) in respondents' homes. The survey should either be face-to-face interviews or by phone, it is not recommended to combine the two approaches.

The national sample of Ukraine consist of **2,389 residents of Ukraine** aged 18 or older and eligible to vote.

The distribution of the population by regions, settlements, and electoral districts is based on statistical data from the latest census and the distribution of the population by gender and age is based on data of the State Statistics Committee of Ukraine 2018 report.

A two-stage probability sampling method is to be used with the random route and next birthday methods for respondent selection.

- Stage One: The territory of Ukraine was split into 25 administrative regions (24 regions of Ukraine and Kyiv). The survey to be conducted throughout all regions of Ukraine.
- Stage Two: the territory of each region to be split into village and city units.

Due to the size of the country both in territory, the number of populations, as well as the size of the cities, the settlements in Ukraine have been further de-constructed to provide more details. Accordingly, the settlements in Ukraine should be split into types by the number of residents:

- Cities with population over 1 million
- Cities with population 500,000-999,000
- Cities with population 100,000-499,000
- Cities with population 50,000-99,000
- Cities with population up to 50,000
- Urban villages
- Villages

Cities and villages to be selected using PPS method (probability proportional to size). The number of selected cities/villages in each of the regions is proportional to the share of population living in cities/villages of a certain type in each region.

All samples to be weighted to be representative with respect to gender and age.

The margin of error should not exceed plus or minus **2.5 percent (maximum level)** for the full sample.

2.3. QUALITATIVE RESEARCH

Following the survey which will provide the quantitative data for the five countries serviced, the qualitative part of the research includes seven focus groups (FGs) for each country, designed to get qualitative feedback from the relevant stakeholders. The focus groups will serve to further understand the quantitative data collected through surveys. Furthermore, focus groups are designed to collect insight and inputs from the more targeted audience which includes also the institutional aspects of cybercrime and cybersecurity.

In each country the research method, research instruments and project structure will be the same.

Qualitative research questions:

1. What is the attitude regarding cybercrimes and cybersecurity topics?
2. What are the main concerns and expectations of the general population regarding cybercrime and cybersecurity?
3. What are the main concerns and expectations of professionals regarding cybercrime and cybersecurity?
4. What are the main differences between professionals and the general population – or 'regular people' – regarding cybercrime and cybersecurity?
5. What are considered to be the most vulnerable groups to cybercrime?

Research universe (target groups):

1. Professionals
2. General population

Qualitative research objectives

There are two sets of objectives for the qualitative research: one for professionals and one for the general population.

In the case of professionals, the main objectives are:

1. Evaluate the levels of **awareness** and types of **knowledge** and **attitudes** professionals have about cybercrime and cybersecurity
2. Identify their main **concerns** and **expectations** regarding cybercrime and cybersecurity
3. Collect **insights**/inputs from cybercrime and cybersecurity specialists about:
 - a. main **types of cybercrime** encountered in their activity (ranking)
 - b. main **causes of cybercrime** (ranking)
4. Identify and evaluate the types of behaviours/**practices** for ensuring cybersecurity (how they fight the cybercrime phenomenon)
5. Identify the main barriers against adopting cybersecurity behaviours/**practices**
6. Identify potential solutions for ensuring cybersecurity in the future (short-term and mid-term)
7. Better understand some of the quantitative data (from the quantitative research report - phase 1), all put in context of that specific country (laws, infrastructure, institutional, private and end-user barriers etc.)

In the case of general population, the main objectives are:

1. Evaluate the levels of **awareness** and types of **knowledge** and **attitudes** members of the general population have about cybercrime and cybersecurity
2. Identify their main **concerns** and **expectations** regarding cybercrime and cybersecurity
3. Collect **insights**/inputs from the general population about:
 - a. main **types of cybercrime** encountered in day-by-day life (ranking)
 - b. main **causes of cybercrime** (ranking)
4. Identify and evaluate the types of behaviours/**practices** for ensuring cybersecurity (how they protect themselves from the cybercrime phenomenon)
5. Identify the main barriers against adopting cybersecurity behaviours/**practices**
6. Better understand the **effects of cybercrime** on the individuals and social groups
7. Better understand some of the quantitative data (from the quantitative research report - phase 1), all put in context of that specific country (laws, infrastructure, institutional, private and end-user barriers etc.)

Research method: Focus Groups (conducted either face-to-face or on-line – video platforms)

Research Instrument: Semi-structured Interview Guide

There will be 5 semi structured Interview Guides:

- 1 FG guide for general population (adults and youngsters)
- 1 FG guide for cybercrime victims
- 1 FG guide for law enforcement officers working in cybercrime
- 1 FG guide for representatives of internet service providers
- 1 FG guide for private company's and NGO's specialists in cybersecurity

Project Structure

Number of focus group sessions: 7 FGs (4 FGs with general population + 3 FGs with professionals)

- 4 FGs with general population
 - 1 FG with adults 22-35 y.o
 - 1 FG with adults 36-65 y.o
 - 1 FG with young people 18-21 y.o
 - 1 FG with victims of cybercrime
- 3 FGs with professionals
 - 1 FG with law enforcement officers working in cybercrime (cybercrime specialists)
 - 1 FG with representatives of internet service providers, mobile and home solutions (cybersecurity specialists)
 - 1 FG with private sector and NGO representatives:
 - private companies' specialists in cybersecurity

- members of IT companies' CSIRT and CERT teams
- representatives of NGOs on human rights

Data collection (depending on the COVID-19 restrictions in each country):

- face-to-face (physical location) or
- on a video platform (online location)

If the FGs will be conducted face-to-face (physical location):

- number of participants: 10
- session duration: approx. 120 minutes (2 hours)
- participants could be recruited from large **or** small cities in each country

If the FGs will be conducted on a video platform (online location):

- number of participants: 8
- session duration: approx. 90 minutes (1.5 hours)
- participants could be recruited from both large **and** small cities in each country

FGs moderator experience: all focus groups will be moderated by a senior researcher, with at least 5 years' experience!

Participant's selection/target groups characteristics:

General population

- 1 FG with adults 22-35 y.o.
 - age: 22-35 y.o
 - 50%-50% mix gender
 - individuals who have mobile or home internet connection
 - individuals who spend at least one hour a day online
- 1 FG with adults 36-65 y.o.
 - age: 36-65 y.o
 - 50%-50% mix gender
 - individuals who have mobile or home internet connection
 - individuals who spend at least one hour a day online
- 1 FG with young people 18-21 y.o.
 - age: 18-21 y.o
 - 50%-50% mix gender
 - Individuals who have mobile or home internet connection
 - Individuals who spend at least one hour a day online
- 1 FG with victims of cybercrime (phishing, ransomware, intimidation and abuse, data breaches & online identity theft)
 - age: 18-65 y.o
 - 50%-50% mix gender
 - at least two victims for each category of category of cybercrime will be present in each group (This recommendation will be updated after receiving the preliminary results from each country, to make sure that for each cybercrime there is a sufficient incidence in the population to make the investigation of that specific crime relevant for the study, and to guarantee the quality of the recruitment process)

Professionals

- 1 FG with law enforcement officers working in cybercrime (cybercrime specialists)
 - age: 22-65 y.o. (active duty)
 - gender balance reflective of the realities in each country's cyber law enforcement environment; typically this might be 70% male - 30% female as opposed to 50% - 50% mix gender
 - professional experience: at least 12 months
 - Law enforcement agent, digital forensics expert, military police officer, private investigator, information technology specialist, or other relevant professional (e.g., an employee in the workforce who is tasked with responding to incidents of cybercrime)

- 1 FG with representatives of internet service providers, mobile and home solutions (cybersecurity specialists)
 - age: 22-65 y.o. (active duty)
 - 50% - 50% mix gender (TBD on the realities in each country)
 - professional experience: at least 12 months
 - Security Analyst, Security Engineer, Security Administrator, Security Consultant/Specialist etc.
- 1 FG with private sector and NGO's representatives (cybersecurity specialists)
 - age: 22-65 y.o. (active duty)
 - 50% - 50% mix gender (TBD on the realities from each country)
 - professional experience: at least 12 months
 - Private company's specialists in cybersecurity (Security Analyst, Security Engineer, Security Architect, Security Administrator, Security Software Developer, Cryptographer/Cryptologist, Cryptanalyst, Chief Information Security Officer, Security Consultant/Specialist etc.)
 - Members of IT companies CSIRTs and CERTs teams (Intrusion Detection Specialist, Computer Security Incident Responder, Virus Technician, Vulnerability Assessors etc.).
 - NGOs on human rights representatives (50% - 50% mix gender)

Recruitment recommendations

For the Face-to-face option (10 participants/session):






- to ensure the presence of 10 participants in each focus group, 14 persons will be recruited (10 participants and 4 reserve participants – 2 for each gender)
- for the age category of 18-21 y.o the age distribution will be as it follows: 18-19 y.o – 5 participants; 20-21 y.o. – 5 participants
- for the age category of 22-35 y.o the age distribution will be as it follows: 22-25 y.o – 3 participants; 26-30 y.o – 3 participants.; 31-35 y.o. – 4 participants
- for the age category of 36-65 y.o the age distribution will be as it follows: 36-40 y.o – 3 participants; 41-45 y.o – 3 participants; 46-50 y.o – 2 participants; 51-65 y.o – 2 participants

For the Video platform (online) option (8 participants/session):

- to ensure the presence of 8 participants in each focus group 12 persons will be recruited (8 participants and 4 reserve participants – 2 for each gender)
- for the age category of 18-21 y.o the age distribution will be as it follows: 18-19 y.o – 4 participants; 20-21 y.o. – 4 participants
- for the age category of 22-35 y.o the age distribution will be as it follows: 22-25 y.o – 3 participants; 26-30 y.o – 2 participants.; 31-35 y.o. – 3 participants
- for the age category of 36-65 y.o the age distribution will be as it follows: 36-40 y.o – 2 participants; 41-45 y.o – 2 participants; 46-50 y.o – 2 participants; 51-65 y.o – 2 participants

3. ANNEXES






Annex 1 – Socio-Demographic Breakdown

	Armenia 	Azerbaijan 	Georgia 	Moldova⁴ 	Ukraine 
	2,959,694	10,067,108	3,716,858	2,640,438 ⁵	41,732,779
Man	1,397,005	5,028,008	1,790,279	1,269,166	19,343,440
Woman	1,562,689	5,039,100	1,926,579	1,371,272	22,389,339
15-19 years	167,710	633,443	205,378	N/A	1,869,743
20-24 years	174,316	723,075	218,346	N/A	2,094,913
25-29 years	235,589	899,404	249,108	N/A	2,728,630
30- 34 years	262,396	932,899	270,180	N/A	3,463,288
35-39 years	239,106	812,876	255,689	N/A	3,455,039
40-44 years	191,772	676,059	676,059	N/A	3,083,056
45-49 years	165,360	613,380	234,113	N/A	2,950,232
50-54 years	162,922	644,922	230,041	N/A	2,695,515
55- 59 years	204,935	645,895	258,783	N/A	3,027,413
60-64 years	190,976	508,569	234,634	N/A	2,831,695
65- 69 years	136,309	299,203	195,518	N/A	2,385,967
Total	72.2	N/A	90.9	75.8	95.5
Man	75.2	N/A	90.5	74.4	93.5
Woman	69.3	N/A	91.4	77.5	97.7
Age 15-64	48.1	68.5	60.6	46.1	61.6
Man	57.7	71.5	66.9	47.1	66.0
Woman	40.0	65.4	54.7	45.2	57.5
Age 15-74	20.5	4.9	12.7	3.0	8.8
Man	20.1	4.1	13.9	3.5	10.0
Woman	21.0	5.8	11.2	2.5	7.4
Youth 15-24	37.2	12.7	29.9	7.4	17.9

⁴ EUROSTAT has no data on Moldova. The data shall be extracted from the national agency

⁵ Data extracted from the National Institute of Statistics of Moldova

Annex 2 – Internet and Social Media Usage

	Armenia 	Azerbaijan 	Georgia 	Moldova 	Ukraine 
% of households 2020	N/A	N/A	83.8%	N/A	71%
% of households 2019	64.7%	79.1%	79.3%	60.8%	65.8%
% of enterprises (10+ employees with internet access)	N/A	63%	98%	N/A	86%
internet use by individuals aged 16-74	N/A	97.3%	72.7%	N/A	78.2%
Man			88.9		47
Woman			89.5		52
15-29 years			95.8		
30-59 years			88.5		
60 years and older			78.7		

Amongst the social media and communication apps that are very popular in all of these five countries are: WhatsApp, Telegram, Facebook, Instagram.⁶

⁶ Confirmed through several sources, including SimilarWeb (30 May 2021).

Annex 3 – Country Profiles

❖ ARMENIA (ARM)

ARMENIA ⁷	
Area	
• Total	29,743 km ²
Population	
• Q3 2020 estimate	2,967,900
• 2011 census	3,018,854
• Density	101.5/km ²
GDP (PPP)	
• Total	2019 estimate \$32.893 billion
• Per capita	\$10,995
GDP (nominal)	
• Total	2019 estimate \$13.444 billion
• Per capita	\$4,527

❖ AZERBAIJAN (AZE)

AZERBAIJAN ⁸	
Area	
• Total	86,600 km ²
Population	
• Q3 2020 estimate	10.2 million
• 2009 census	8,9 million
• Density	123/km ²
GDP (PPP)	
• Total	2019 Estimate \$144, 374 billion
• Per capita	\$14,403
GDP (nominal)	
• Total	2019 Estimate \$ 48.05 billion
• Per capita	\$5,880

⁷ CIA (2021, April). Armenia Country Profile. Retrieved May, 2021, from <https://www.cia.gov/the-world-factbook/static/1852cd699f3c2745498eab22dba758a4/AM-summary.pdf>; Statistical Committee of the Republic of Armenia (2021). Statistical Data. Retrieved 2021, from <https://www.armstat.am/en/>; World Banks (2021). GDP, PPP (current international) - Armenia. Retrieved from <https://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD?locations=AM&view=chart>; Trading Economics (2021). Armenia - Economic Indicators. Retrieved 2021, from <https://tradingeconomics.com/armenia/indicators>; International Monetary Fund (2021). Republic of Armenia and the IMF. Retrieved 2021, from <https://www.imf.org/en/Countries/ARM>

⁸ CIA (2021). Azerbaijan Country Profile. Retrieved 2021, from <https://www.cia.gov/the-world-factbook/static/062dd536f41a81a307b1f2cd360fdc9f/AJ-summary.pdf>; The State Statistical Committee of the Republic of Azerbaijan (2021). Retrieved 2021, from <https://www.stat.gov.az/?lang=en>; Trading Economics (2021). Azerbaijan - Economic Indicators. Retrieved 2021, from <https://tradingeconomics.com/azerbaijan/indicators>; World Bank (2021). Azerbaijan Country Data. Retrieved 2021, from <https://data.worldbank.org/country/azerbaijan?view=chart>.

❖ GEORGIA (GEO)

GEORGIA ⁹	
Area	
• Total	69,700 km ²
Population	
• Q3 2020 estimate	4 million
• 2019 census	3.72 million
• Density	65/km ²
GDP (PPP)	
• Total	2019 \$15,65 billion
• Per capita	\$10,700
GDP (nominal)	
• Total	2019 \$ 17.74 billion
• Per capita	\$4,986

❖ MOLDOVA (MDA)

MOLDOVA ¹⁰	
Area	
• Total	33,851 km ²
Population	
• Q3 2020 estimate	4 million
• 2014 census	2.8 million
• Density	98.3/km ²
GDP (PPP)	
• Total	2019 \$ 27.282 billion
• Per capita	\$13,033.00
GDP (nominal)	
• Total	2019 \$ 11.96 billion
• Per capita	\$3,715

⁹ CIA (2021). Georgia Country Profile. Retrieved 2021, from <https://www.cia.gov/the-world-factbook/countries/georgia/>; W. (2021). GDP per capita, PPP (current international \$) - Georgia. Retrieved 2021, from <https://data.worldbank.org/indicator/NY.GDP.PCAP.PP.CD?locations=GE>; Trading Economics, Georgia Economic Data. (2021). Retrieved 2021, from <https://tradingeconomics.com/georgia/indicators>;

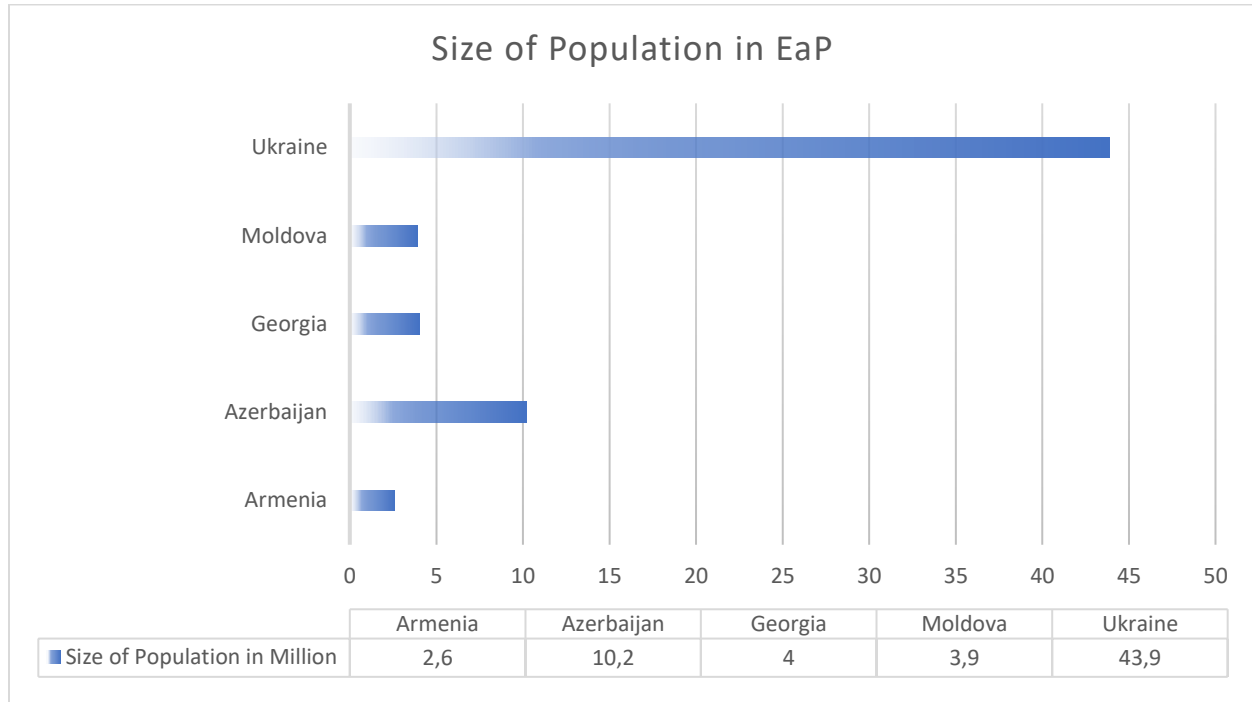
¹⁰ The National Bureau of Statistics (2021). // Population and Housing Census in 2014. Retrieved 2021, from <https://statistica.gov.md/pageview.php?l=en&idc=479>; CIA (2021). Moldova Country Profile. Retrieved 2021, from <https://www.cia.gov/the-world-factbook/static/70c2831b6c7b40fc546858a6c55e2d5/MD-summary.pdf>, World Bank (2021). Moldova Economic Data. Retrieved 2021, from <https://data.worldbank.org/country/moldova?view=chart>.

❖ UKRAINE (UKR)

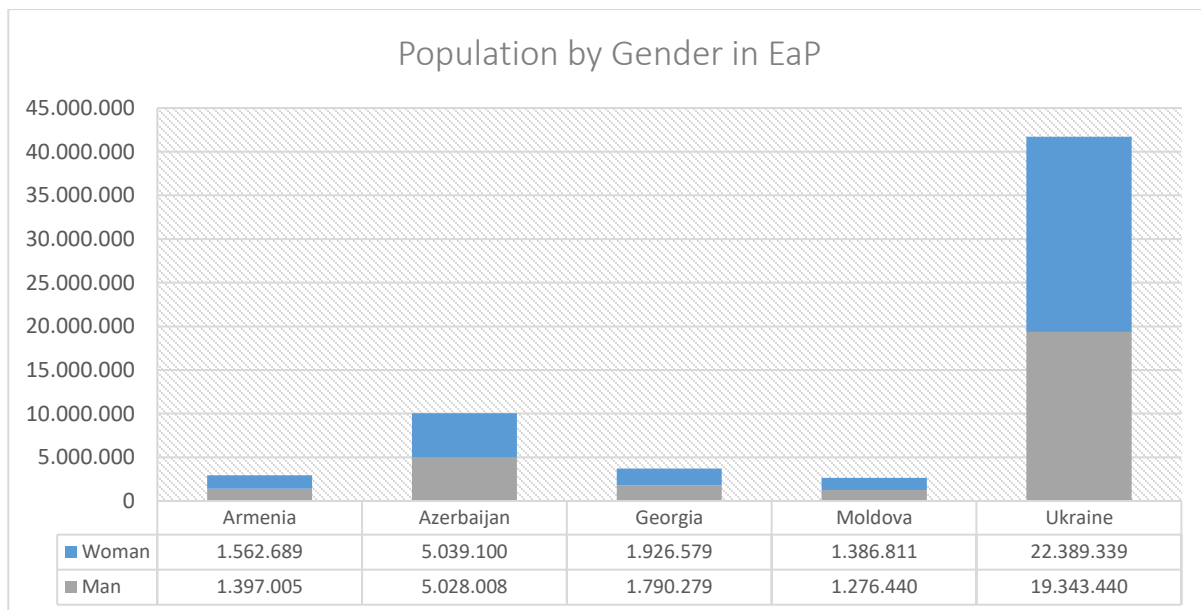
UKRAINE ¹¹	
Area	
• Total	603,550 km ²
Population	
• Q3 2020 estimate	43.9 million
• 2001 census	48.4 million
• Density	80/km ²
GDP (PPP)	
• Total	2019
• Per capita	\$526,2 billion (2020)
• Per capita	\$12,810.00
GDP (nominal)	
• Total	2019
• Total	\$153.8 billion
• Per capita	\$3,225

¹¹ Ministry of Development and Trade – Ukraine (2021). Ukraine Country Profile. Retrieved 2021, from http://ukrexport.gov.ua/eng/about_ukraine/population/ukr/179.html; Ukraine: Total number of actual population.: (2021). Retrieved 2021, from <http://2001.ukrcensus.gov.ua/eng/results/general/estimate/>; Ukraine Economic Data. World Bank (2021). Retrieved 2021, from <https://data.worldbank.org/country/ukraine?view=chart>.

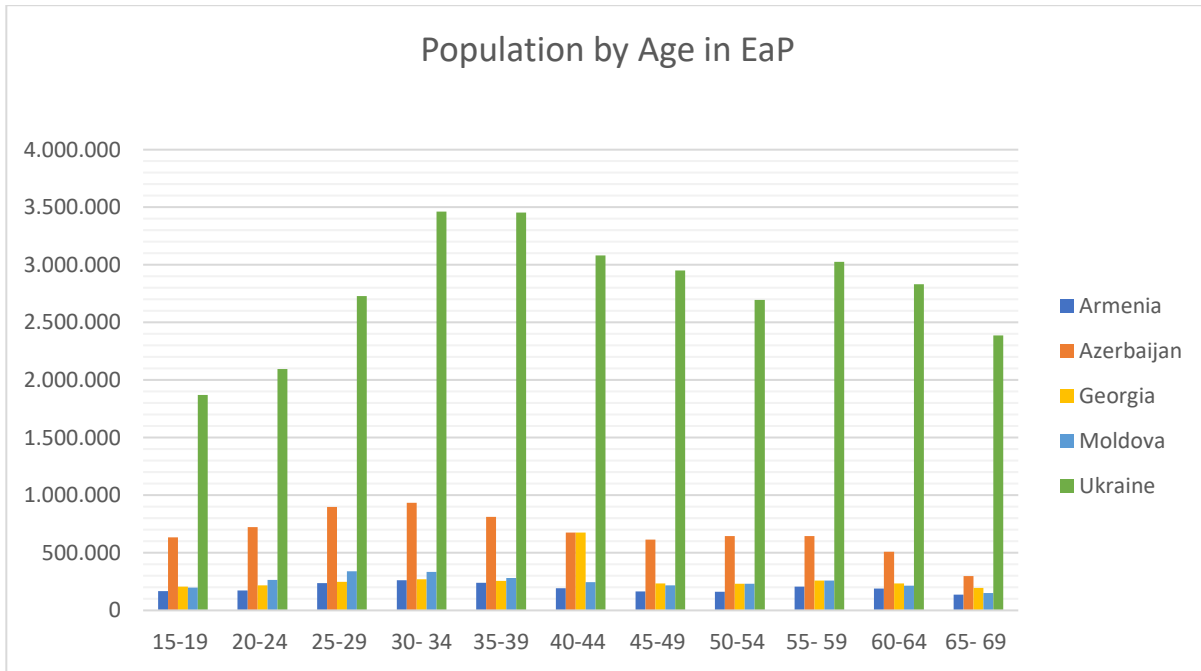
Annex 4 – EaP comparative profiles



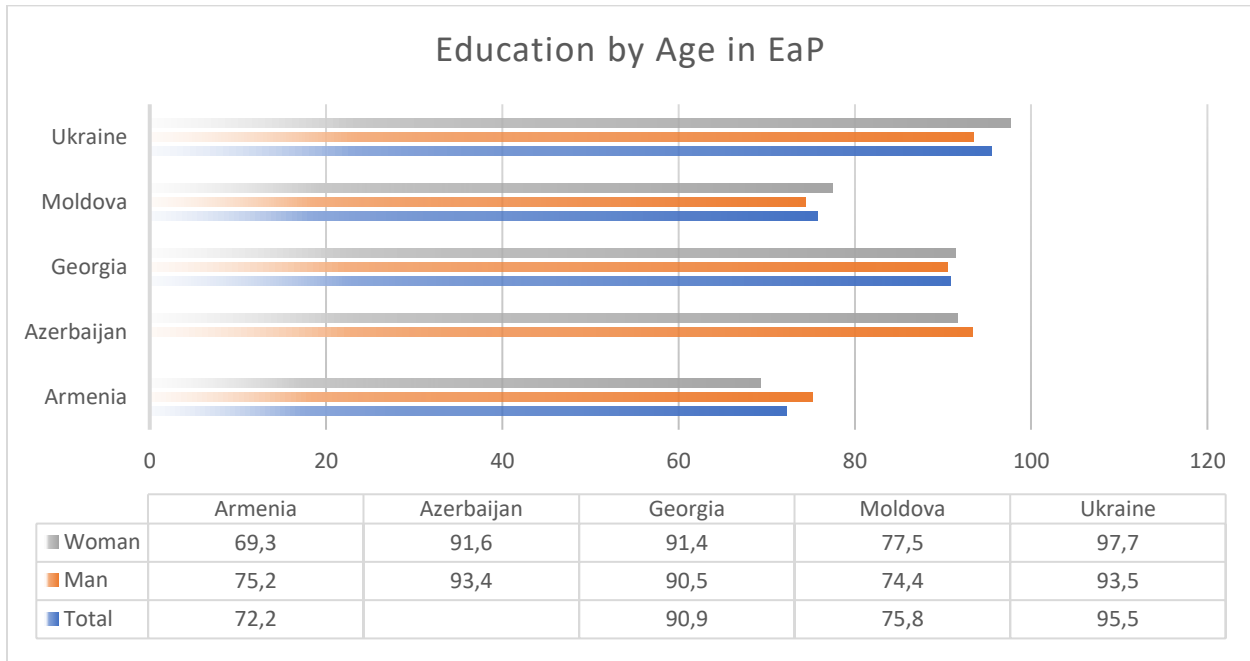
Graph 4. Population in EaP in million



Graph 5. Population by Gender in EaP



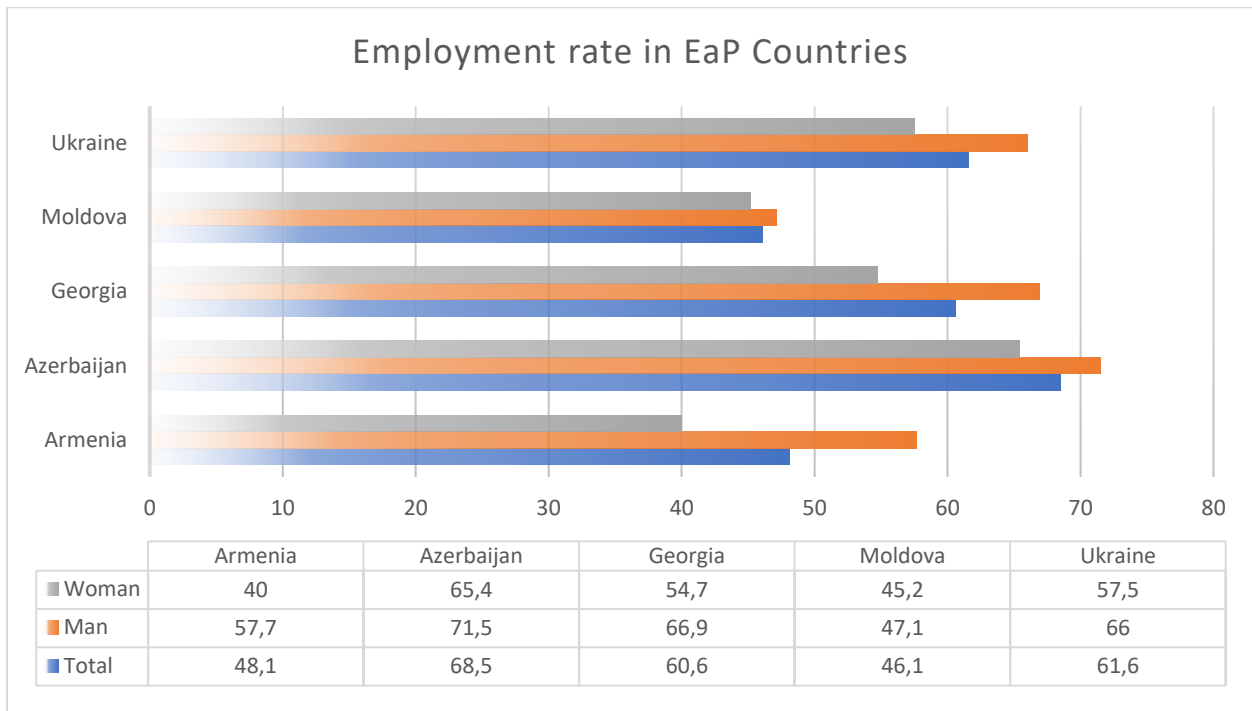
Graph 6. Population by Age in EaP¹²



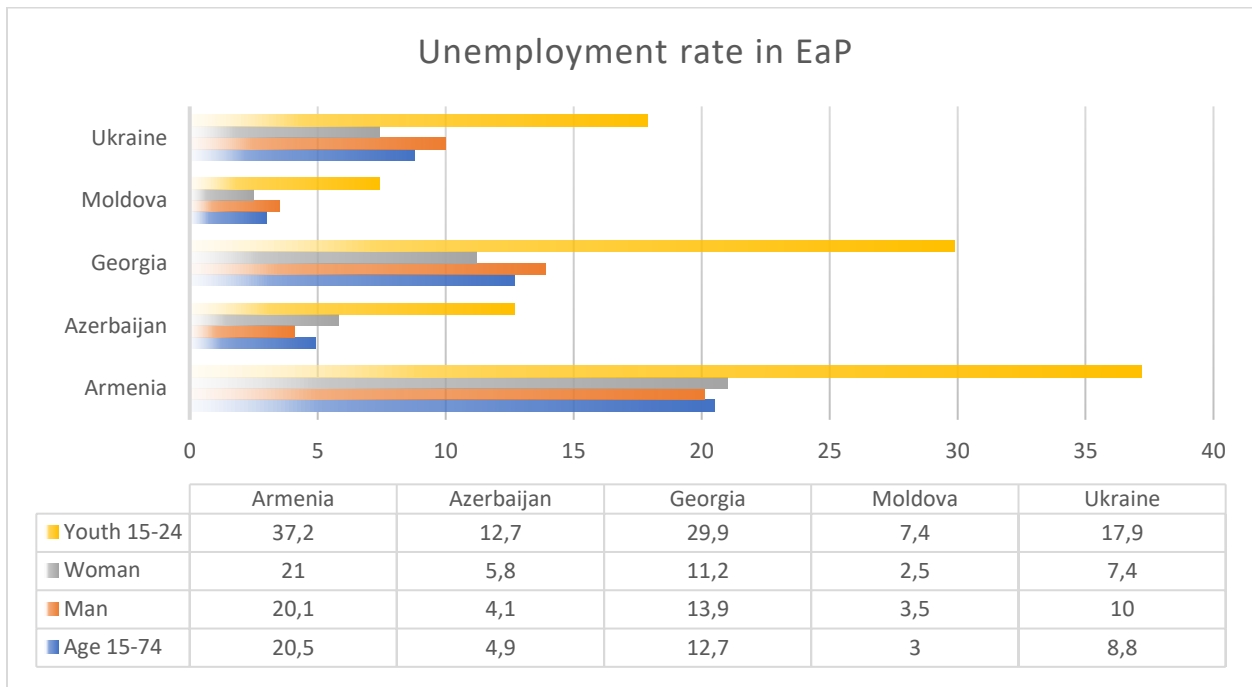
Graph 7. Education by Age in EaP¹³

¹² Data for Moldova is from 2017, whereas for other countries from 2019.

¹³ According to Eurostat, Azerbaijan data recorded is from 2009. No recent data on educational attainment is available for Azerbaijan.



Graph 8. Employment Rate in EaP



Graph 9. Unemployment rate in EaP

Annex 5 – Country Cyber State of Play






	ARM 	AZE 	GEO 	MDA 	UKR 
NIS Directive	No	N/A	Planned	Planned	No
National Cybersecurity Strategy	None: Strategy prepared in 2017 but not yet adopted & implemented	Adopted in late May 2019	Expired: A new strategy is pending final inputs by the NSC and will be sent for adoption	Adopted with National Cybersecurity Plan within National Information Security Strategy	Adopted
National CERT	cert.am	cert.gov.az/en & cert.az	cert.gov.ge	stisc-cert.gov.md/?lang=en	cert.gov.ua
CI & CII & OES Lists	No	CI only	CII only	CI only	No
National Risk Assessment Methodology	No	Yes Chapter in the National Cyber Security Strategy (2020-2025)	Partly: Cyberthreats addressed only	No	No
National Incident Reporting Mechanism	No	Yes	Yes	No	No
Cybercrime in National Law	Yes	Yes	Yes	Partly	Partly

Table 1. Comparison of state-of-play across all partner countries

Annex 6 – Survey: Questionnaire for Individuals

This questionnaire for individuals contains a total of 60 questions – introduction framing, core and demographic questions – and is aimed at private citizens of EaP countries. It draws from the Budapest Convention¹⁴ (art. 2-8)¹⁵ and its First Additional Protocol¹⁶ (art. 3-5)¹⁷, especially where they are aimed at protecting individuals. Its further aim is to allow comparison to Europol's 2020 IOCTA.

The questionnaire is to be pre-empted by lead-in questions to establish a rapport with the interviewee and to gauge their personal cybersecurity posture as well as their attitude towards cybercrime.

Framework definition and intro (incl. GDPR provisions – to be adapted after local needs)

First of all, thank you for accepting to take part in this research. The purpose of this research project is to collect data on national attitudes towards cybersecurity and cybercrime. This is a research activity being conducted in the framework of the Cyber East and Cybersecurity East project, a joint activity of the Council of Europe and the European Union.

Your participation in this survey is voluntary. You can choose not to participate. If you decide to participate in this survey, you have the option of withdrawing at any time. The procedure involves providing answers to the survey questions that will take approximately 30 – 40 minutes.

The projects will treat all personal information with strict confidentiality and in accordance with EU's General Data Protection Regulation (GDPR) and national data protection legal framework.

Only the company and the projects that collect data will have temporary access to your contact information. Your name and other contact information will be deleted before the survey data is published and no later than 2 February 2022.

All your responses are confidential. Any personal identification data is stored separately from the rest of your responses. Rest assured: these results are only used on an aggregate level and for research purposes only. There is no link between your answers and your identity!

Results of the surveys will be shared only with your respective country (regional publication will be discussed separately) and are meant to be used to further contribute to other reporting efforts (e.g. IOCTA) as well as for shaping future policies, strategies and capacity building responses on cybercrime, cybersecurity and electronic evidence in the near and mid-term.

If you agree with these conditions, please check (or say) YES to proceed. Thank you very much!

Technographics intro

1. Do you or anyone in your household have access to the internet at home? **DO NOT READ**
 - a. Yes
 - b. No
 - c. Not Sure
 - d. DK / NA

¹⁴ Signatories: Armenia (2007), Azerbaijan (2010), Georgia (2012), Republic of Moldova (2009), Ukraine (2006)

¹⁵ Armenia has deposited a declaration regarding article 4 and this has been taken into account in development

¹⁶ Signatories: Armenia (2007), Republic of Moldova (2017), Ukraine (2007)

¹⁷ Ukraine has deposited a declaration regarding article 6, this article is not covered by this questionnaire

2. Do you regularly use for personal needs any of the following devices? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
- Smartphone
 - Tablet
 - Laptop
 - Desktop
 - Smart TV
 - Game Console
 - Other: [...] **WRITE DOWN ANSWER**
 - DK / NA
3. How much of your *personal time in a day do you spend on your devices*, whether or not they are online – please estimate the total time for all – smartphone, tablet, computers? **OPEN ANSWER IN HRS**
- [.....] **WRITE DOWN ANSWER**
4. How much of your *personal time in a day do you spend ONLINE on your devices* – please estimate the total time for all – smartphone, tablet, computers? **OPEN ANSWER IN HRS**
- [.....] **WRITE DOWN ANSWER**
5. What are the activities you do online regularly? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
- COMMUNICATION
- Sending / receiving E-mail
 - Making calls (including video calls) over the internet, for example, via Skype, Messenger, WhatsApp, Facetime, Viber, Snapchat
 - Participating in social networks (creating user profile, posting messages or other contributions to Facebook, Twitter, Instagram, Snapchat, etc.)
- ACCESS TO INFORMATION
- Finding information about goods, work or services
 - Reading online news sites / newspapers / news magazines
- CREATIVITY
- Sharing or publishing self-created videos, photos, music, texts etc. on a website or via app
- USE OF ENTERTAINMENT
- Listening to music (music streaming) or downloading music
 - Watching internet-streamed TV (live or catch-up) from TV broadcasters (e.g. [national examples])
 - Watching Video on Demand from commercial services (e.g. Netflix, HBO GO, Amazon Prime etc)
 - Watching video content from sharing services (e.g. YouTube)
 - Playing or downloading games
- OTHER ON-LINE SERVICES
- Selling of goods or services via a website or app
 - Online Banking
 - E-government services

General Usage and Attitudes 1

6. Are you familiar with the word cybercrime?
- Yes
 - No

- c. Not Sure
- d. DK / NA

For this interview, *cybercrime* refers to the criminal activity that either targets or abuses a computer, a computer network, or a networked device.

7. After hearing this definition, please tell us with which of these statements do you agree more:
- a. Cybercrime is rather rare and usually happens predominantly to businesses and / or individuals that are somehow involved with dubious activities; it is not a serious risk for 'normal' people.
 - b. Cybercrime is a real threat to people's welfare and wellbeing and nowadays everyone is at risk at becoming a target.
8. What do you generally do to protect yourself from cybercrime? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-c**
- a. I am being careful with what I do when I am using my devices – e.g., do not open suspicious mail etc. **CONTINUE @ 9**
 - b. I restrict access to my devices – e.g., using passwords etc. **CONTINUE @ 10**
 - c. I use security software – e.g., antivirus/anti-malware etc. **CONTINUE @ 11**
 - d. None of the above
 - e. Not sure
 - f. DK / NA
9. **ASK ONLY FOR 8.a** Which of the following behaviors do you employ regularly when you are careful when using your devices **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-f**
- a. I delete suspicious messages
 - b. I open suspicious messages, but I do not reply to them and do not click on their contents if they do not seem authentic
 - c. I avoid / do not use suspicious sites
 - d. I avoid / do not use sites that may be involved in distributing illegal or pirated content
 - e. I avoid / refuse giving any of my personal data to third parties
 - f. I do not use free wireless networks
 - g. None of the above
 - h. Not sure
 - i. DK / NA
10. **ASK ONLY FOR 8.b** How do you usually restrict access to your personal devices **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-d**
- a. Password
 - b. PIN
 - c. Biometrics – fingerprint, face recognition
 - d. Two-factor authentication
 - e. None of the above
 - f. Not sure
 - g. DK / NA
11. **ASK ONLY FOR 8.c** On what devices do you currently have security software installed **READ CHOICES, MULTIPLE ANSWERS ACCEPTED for a-d**
- a. Smartphone
 - b. Tablet
 - c. Laptop
 - d. Desktop

- e. None of the above
 - f. Not sure
 - g. DK / NA
12. **ASK ONLY FOR 8.d** Is there a reason why you don't use any of these means of protection from cybercrime? (If so: what is the reason?) **OPEN ANSWER**
- a. [.....] **WRITE DOWN ANSWER**
13. Have you ever been targeted by an attempt of what you felt, then, was computer / online criminal activity?
- a. Yes
 - b. No
 - c. DK / NA
14. Do you feel that the COVID-19 pandemic has exacerbated cybercrime against citizens of [country]?
- a. Yes
 - b. No
 - c. DK / NA

Phishing

15. Over the past 12 months, have you been contacted by someone *pretending* to be a representative of a technology company, with an offer of live service?
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA
16. Are you familiar with the word *phishing*?
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA

For this interview, *phishing* is when criminals use remote contacting to impersonate other parties – through phone, e-mail, text messages or social networks. The criminals pretend to be someone else and will attempt to trick the recipient into installing malicious software or sending them money or private information.

17. After hearing this definition, have you ever *heard* of this type of crime happening?
- a. Yes
 - b. No **CONTINUE @ 21**
 - c. Not sure
 - d. DK / NA
18. Over the past 12 months, have you received any *phishing message or call*?
- a. Yes
 - e. No **CONTINUE @ 21**
 - b. Not sure
 - c. DK / NA

19. Please indicate in which of the following ways you may have received any phishing messages over the past 12 months, on any of your *personal* devices or accounts? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED**
- e-mail
 - text message on phone (sms, iMessage)
 - app conversation on phone (for example, WhatsApp, Telegram)
 - social media (for example, Facebook, Instagram)
 - voice or video call
 - unanswered call from a strange number (trying to get recipient to call back)
 - other [...] **WRITE DOWN ANSWER**
20. Over the past 12 months, have you ever trustingly engaged with such a message? *This could mean: have a trusting conversation with the originator, but also clicking on a link or installing software they sent.* **READ CHOICES**
- Yes
 - No
 - Not sure
 - I would rather not talk about it
 - DK / NA
21. On a scale of 1 to 4, how deeply has phishing (as discussed before) affected your life over the past 12 months? **READ CHOICES**
- 1 = not affected me at all
 - 2 = it has been a nuisance
 - 3 = it has distressed me
 - 4 = it has negatively impacted my life
 - DK / NA
22. If someone in your neighborhood would receive such a phishing message, and perhaps trustingly engage with it, do you think they would report it to the [authorities/police]. **READ CHOICES**
- Yes, I think they would
 - Yes, but only the serious cases
 - No, they would not report it
 - Not sure
 - DK / NA
23. Which one of the following better describes how you feel about the phishing criminal activities here in [country]? **READ CHOICES**
- 1 = Dismissive
 - 2 = Doubtful
 - 3 = Disengaged
 - 4 = Cautious
 - 5 = Concerned
 - 6 = Alarmed
 - DK / NA
24. 11) Do you feel you know enough about phishing to protect yourself and your family? **READ CHOICES**
- Yes
 - No

- c. Not sure
- d. DK / NA

Ransomware

25. Are you familiar with the word *ransomware*?
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA

For this interview, *ransomware* is an illegal application that criminals use to block access to computers, mobile phones and to the data and photos that they may contain. The criminals will then ask the victim for money to release the computer, mobile phone, data or photos.

26. After hearing this definition, have you ever *heard* of this type of crime happening?
- a. Yes
 - b. No **CONTINUE @ 29**
 - c. Not sure
 - d. DK / NA

27. Do you personally know anyone who, over the past 12 months, has fallen victim to ransomware?
- a. Yes, someone in my family
 - b. Yes, someone else I know
 - c. Yes, it happened to me
 - d. No **CONTINUE @ 29**
 - e. Not sure **CONTINUE @ 29**
 - f. I would rather not say **CONTINUE @ 29**
 - g. DK / NA

28. I am sorry to hear this. I have one very technical question about this, most people are not able to answer this. Do you happen to know the type(s) of ransomware involved? **OPEN ANSWER**

- a. [.....] **WRITE DOWN ANSWER**

29. Let's imagine a *ransomware attack* happened to someone in your neighborhood and they lost access to their computer, their mobile phone, or to the data or photos that they contained. Do you think the victim would report it to the [authorities/police]? **READ CHOICES**
- a. Yes, I think they would
 - b. Yes, but only the serious cases
 - c. No, they would not report it
 - d. Not sure
 - e. DK / NA

30. Let's say for a minute, that a ransomware attack happened to you. Your favorite computer, phone, data or photos would be permanently inaccessible, unless you pay a significant amount of money. On a scale of 1-4, how deeply would this affect you? **READ CHOICES**
- a. 1 = not affected me at all
 - b. 2 = it has been a nuisance
 - c. 3 = it has distressed me
 - d. 4 = it has negatively impacted my life

e. DK / NA

31. Which one of the following better describes how you feel about the ransomware criminal activities here in [country]? **READ CHOICES**

- a. 1 = Dismissive
- b. 2 = Doubtful
- c. 3 = Disengaged
- d. 4 = Cautious
- e. 5 = Concerned
- f. 6 = Alarmed
- g. DK / NA

32. 11) Do you feel you know enough about ransomware to protect yourself and your family?

READ CHOICES

- e. Yes
- f. No
- g. Not sure
- h. DK / NA

Intimidation and abuse

I have a few questions in front of me about online intimidation and abuse. I won't ask about any details. Still, please don't feel any obligation to answer.

33. Would you be willing to answer a few questions about intimidation and abuse? **READ**

CHOICES

- e. Yes
- f. No **CONTINUE @ 39**
- g. Not sure
- h. DK / NA

34. Some online interactions can be very *intimidating*. Has anyone that you personally know been *insulted, bullied, blackmailed, or intimidated* online, in the past 12 months?

- a. Yes, someone in my family
- b. Yes, someone else I know
- c. Yes, it happened to me
- d. No
- e. Not sure
- f. I would rather not say
- g. DK / NA

35. In the past 12 months, have you yourself witnessed any online promotion of *hatred, discrimination, or violence* against people of a certain race, color, descent or origin?

- h. Yes
- i. No
- j. Not sure
- k. I would rather not say
- l. DK / NA

36. Unfortunately, the internet can sometimes be an unsuitable place for *minors*. Do you think [the authorities / law enforcement] should do more to protect them online? **READ CHOICES**

- a. Yes

- b. No
 - c. Not sure
 - d. I would rather not say
 - e. DK / NA
37. I have asked you a few questions about online intimidation and abuse. If someone in your neighborhood fell victim to such crimes, do you think they would report it to the [authorities/police]? **READ CHOICES**
- a. Yes, I think they would
 - b. Yes, but only the serious cases
 - c. No, they would not report it
 - d. Not sure
 - e. DK / NA
38. On a scale of 1 to 4, how deeply have online intimidation or abuse affected your life over the past 12 months? **READ CHOICES**
- a. 1 = not affected me at all
 - b. 2 = it has been a nuisance
 - c. 3 = it has distressed me
 - d. 4 = it has negatively impacted my life
 - e. DK / NA
39. Which one of the following better describes how you feel about the ransomware criminal activities here in [country]? **READ CHOICES**
- h. 1 = Dismissive
 - i. 2 = Doubtful
 - j. 3 = Disengaged
 - k. 4 = Cautious
 - l. 5 = Concerned
 - m. 6 = Alarmed
 - n. DK / NA
40. Do you feel you know enough about online intimidation and abuse to protect yourself and your family? **READ CHOICES**
- i. Yes
 - j. No
 - k. Not sure
 - l. DK / NA

Interference (services made unavailable)

Sometimes, online services can be unreachable due to a malfunction. At other times, criminals are blocking access to them.

41. In the past 12 months, has any of the online services that you rely on been unexpectedly unreachable for a prolonged time? **READ CHOICES**
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA
 - m. DK / NA

Data breaches and online identity theft

42. In the past 12 months, have you become aware that *login credentials* to a *personal account of yours had been exposed* online?
- Yes
 - No
 - Not sure
 - DK / NA
43. In the past 12 months, have you become aware that a *personal account of yours had been accessed, or it was attempted*, by anyone you did not mean to access it?
- Yes, and they succeeded
 - It was attempted but they failed
 - No
 - Not sure
 - DK / NA
44. In the past 12 months, have you become aware that any *personal data of yours had been deliberately and illegally exposed* online?
- Yes
 - No
 - Not sure
 - DK / NA
45. In the past 12 months, have you become aware that any *personal data of yours had been abused, or it was attempted*?
- Yes, and they succeeded
 - It was attempted but they failed
 - No
 - Not sure
 - DK / NA
46. In the past 12 months, have you become aware that any of your *bank accounts, online payment accounts or credit card details had been exposed* online?
- Yes
 - No
 - Not sure
 - DK / NA
47. In the past 12 months, have you become aware that any of your *bank accounts, online payment accounts or credit card details had been abused by a stranger, or it was attempted*?
- Yes, and they succeeded
 - It was attempted but they failed
 - No
 - Not sure
 - DK / NA
48. In the past 12 months, have you become aware that your *personal mobile phone number* had been taken over by someone you did not mean to have access to it?
- Yes, and they succeeded
 - It was attempted but they failed

- c. No
 - d. Not sure
 - e. DK / NA
49. In the past 12 months, have you found that a phone number or online account of *someone you already knew* had been taken over, and this person was being impersonated when the account was communicating with you?
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA
50. We have discussed several ways criminals can try to pretend they are someone else. This is called *online identity theft* and it is a major component in cybercrime. If someone in your neighborhood falls victim to online identity theft, or to a scam abusing a stolen identity, do you think they would report it to the [authorities/police]. **READ CHOICES**
- a. Yes, I think they would
 - b. Yes, but only the serious cases
 - c. No, they would not report it
 - d. Not sure
 - e. DK / NA
51. On a scale of 1 to 4, how deeply has online identity theft affected your life over the past 12 months? **READ CHOICES**
- a. 1 = not affected me at all
 - b. 2 = it has been a nuisance
 - c. 3 = it has distressed me
 - d. 4 = it has negatively impacted my life
 - e. DK / NA
52. Which one of the following better describes how you feel about the online identity theft here in [country]? **READ CHOICES**
- a. 1 = Dismissive
 - b. 2 = Doubtful
 - c. 3 = Disengaged
 - d. 4 = Cautious
 - e. 5 = Concerned
 - f. 6 = Alarmed
 - g. DK / NA
53. Do you feel you know enough about online identity theft to protect yourself and your family?
READ CHOICES
- a. Yes
 - b. No
 - c. Not sure
 - d. DK / NA

General Usage and Attitudes 2

54. Now that we have discussed all these types of cybercrime which one would you say it worries you most? **READ CHOICES**
- a. Phishing

- b. Ransomware
 - c. Online intimidation and abuse
 - d. Interference (services made unavailable)
 - e. Data breaches and online identity theft
 - f. DK / NA
55. Comparing cybercrime with other types of crime present in our society please tell us which one worries you most? What about the one that worries you the least? **READ CHOICES, RANDOMIZE LIST**
- a. Cybercrime
 - b. Violent crime – e.g., robbery, assault etc.
 - c. Property crime – e.g., burglary, auto-theft etc.
 - d. White collar crimes (excluding cybercrime) - e.g., fraud, bribery etc.
56. On a scale of 1 to 4, how prepared do you feel are the authorities in your country to take on cybercrime?
- a. 1 = not ready
 - b. 2 = rather unprepared
 - c. 3 = prepared but still work to do
 - d. 4 = very prepared
 - e. DK / NA
57. Looking at the next 5 years do you expect the cybercrime activities to?
- a. Decrease drastically
 - b. Relatively decrease
 - c. Relatively increase
 - d. Increase drastically
 - e. DK / NA

Demographics fade out

58. Are you male or female?
- a. Male
 - b. Female
59. What is your age? **DO NOT READ**
- a. 18-20
 - b. 21-24
 - c. 25-29
 - d. 30-34
 - e. 35-39
 - f. 40-44
 - g. 45-49
 - h. 50-54
 - i. 55-59
 - j. 60-64
 - k. 65+
60. What is highest level of education you have completed? **READ CHOICES**
- a. No qualifications
 - b. Middle school
 - c. High school

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe



Cybersecurity EAST

- d. Bachelor's Degree
- e. Master's Degree
- f. Doctoral studies
- g. Postdoctoral studies
- h. Don't know /prefer not to say **DO NOT READ**

Annex 7 – Survey: Questionnaire for Enterprises

This questionnaire for enterprises contains a total of 46 questions.

The questionnaire is to be pre-empted by lead-in questions to establish a rapport with the interviewee and to gauge their company cybersecurity posture as well as their attitude towards cybercrime.

Framework definition and intro (incl. GDPR provisions – to be adapted after local needs)

First of all, thank you for accepting to take part in this research. The purpose of this research project is to collect data on national attitudes towards cybersecurity and cybercrime. This is a research activity being conducted in the framework of the Cyber East and Cybersecurity East project, a joint activity of the Council of Europe and the European Union.

Your participation in this survey is voluntary. You can choose not to participate. If you decide to participate in this survey, you have the option of withdrawing at any time. The procedure involves providing answers to the survey questions that will take approximately 30 – 40 minutes.

The projects will treat all personal information with strict confidentiality and in accordance with EU's General Data Protection Regulation (GDPR) and national data protection legal framework.

Only the company and the projects that collect data will have temporary access to your contact information. Your name and other contact information will be deleted before the survey data is published and no later than 2 February 2022.

All your responses are confidential. Any personal identification data is stored separately from the rest of your responses. Rest assured: these results are only used on an aggregate level and for research purposes only. There is no link between your answers and your identity!

Results of the surveys will be shared only with your respective country (regional publication will be discussed separately) and are meant to be used to further contribute to other reporting efforts (e.g. IOCTA) as well as for shaping future policies, strategies and capacity building responses on cybercrime, cybersecurity and electronic evidence in the near and mid-term.

If you agree with these conditions, please check (or say) YES to proceed. Thank you very much!

Organizational Intro & Info

- 1) In which sector is your company active? **READ CHOICES**
 - Finance
 - Telecommunication
 - Energy
 - Automotive
 - Logistics and Transport
 - Manufacturing
 - Retail
 - Information Technology (Hardware, Software, Services)
 - Food
 - Healthcare
 - Real Estate
 - Other [...] **WRITE DOWN ANSWER**
 - DK / NA

- 2) Do all the persons employed in your company/enterprise have access to the internet for business purposes? (this includes a fixed line and/or a mobile connection) **DO NOT READ**

- a. Yes
 - b. No
 - c. DK / NA
- 3) Does your company/enterprise use any type of fixed line connection to the internet? (ADSL, SDSL, VDSL, fiber optics technology (FTTP), cable technology, etc.) **DO NOT READ**
- a. Yes
 - b. No
 - c. DK / NA
- 4) What is the maximum contracted download speed of the fastest fixed-line internet connection of your enterprise? **READ CHOICES**
- a. less than 30 Mbit/s
 - b. at least 30 but less than 100 Mbit/s
 - c. at least 100 Mbit/s but less than 500 Mbit/s
 - d. at least 500 Mbit/s but less than 1 Gbit/s
 - e. at least 1 Gbit/s
 - f. Not sure
 - g. DK / NA
- 5) Does your enterprise allow a mobile connection to the internet using mobile telephone networks, for business purposes? **DO NOT READ**
- a. Yes
 - b. No
 - c. DK / NA
- 6) Does your enterprise use any of the following online tools? **READ CHOICES**
- a. A corporate website
 - b. Social networks (e.g., LinkedIn, Facebook, Odnoklassniki, Vkontakte, Xing, etc.)
 - c. Enterprise's blog or microblogs (e.g., Twitter, etc.)
 - d. Multimedia content sharing websites or apps (e.g., YouTube, Flickr, SlideShare, Instagram, Pinterest, Snapchat etc.)
 - e. Wiki based knowledge sharing tools
 - f. Other: [...] **WRITE DOWN ANSWER**
 - g. **DK / NA**

Cybersecurity role

- 7) Does your company have a dedicated organizational role / department in charge of cybersecurity? **READ CHOICES**
- a. Yes, a dedicated department
 - b. Yes, but as part of another department
 - c. Yes, one or two job roles
 - d. Other, please specify
 - e. No
 - f. DK / NA
- 8) Does your company (also) outsource some of the services needed to manage cybersecurity? **READ CHOICES**
- a. Yes, some elements that cannot be covered inhouse
 - b. Yes, all cybersecurity issues

- c. No
d. DK / NA
- 9) Approximately, what percentage of your IT-budget was spent on cybersecurity in the last 12 months? **READ CHOICES**
- a. 0 - 5%
 - b. 5 - 10%
 - c. 10 - 20%
 - d. > 20%
 - e. Not sure
 - f. I would rather not say
 - g. DK / NA
- 10) What is your yearly spending on cybersecurity insurance(s) in percentage of your IT-budget?
READ CHOICES
- a. have no cybersecurity insurance
 - b. 0 - 5%
 - c. 5 - 10%
 - d. 10 - 20%
 - e. > 20%
 - f. Not sure
 - g. I would rather not say
 - h. DK / NA
- 11) Does your company follow any security frameworks or standards? **READ CHOICES, MULTIPLE ANSWERS**
- a. ISO 27000
 - b. ITIL
 - c. COBIT
 - d. Other [...] **WRITE DOWN ANSWER**
 - e. Not sure
 - f. I would rather not say
 - g. DK / NA
- 12) Which of the following does your business currently use? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. Website for your business
 - b. Social media accounts for your business
 - c. E-commerce platforms and solutions
 - d. Web-based application
 - e. Open-source software
 - f. Cloud computing or storage
 - g. Internet-connected smart devices or Internet of Things (IoT)
 - h. Intranet
 - i. Blockchain technologies
 - j. Cryptocurrencies (such as bitcoin)
 - k. Voice over Internet Protocol (VoIP) services
 - l. Video / live communication and conferencing
 - m. Business does not use any of the above
 - n. DK / NA
- 13) What type of data does your business store – on cloud computing or storage services? Include data that are backed-up. **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. Confidential employee information
 - b. Confidential information about customers, suppliers, partners or other third parties

- c. Confidential business information
 - d. Commercially sensitive information
 - e. Non-sensitive or public information
 - f. Business does not store data on cloud computing or storage services
 - g. DK / NA
- 14) Does anyone in your business use personally owned devices such as smartphones, tablets, laptops, or computers to carry out regular business-related activities? **READ CHOICES**
- a. Yes, all the time
 - b. Yes, but rarely, as an exception
 - c. No
 - d. No, and this is explicitly forbidden by company policy
 - e. DK / NA

General Priority and Confidence

- 15) How do you rank cybersecurity within your company? **READ CHOICES**
- a. Cyber-attacks are the top risk for my company
 - b. Cyber-attacks are among the 5 the top risks for my company
 - c. Cyber-attacks are a low risk for my company
 - d. Cyber-attacks are not at all a risk for my company
 - e. DK / NA
- 16) What are your critical areas of cybersecurity? **READ CHOICES, MULTIPLE ANSWERS**
ACCEPTED FOR a-c
My company is:
- a. understanding and assessing cyber risks
 - b. preventing cyber threats from being realized
 - c. responding to and recovering from cyber events
 - d. not affected by cyber risks
 - e. DK / NA
- 17) Which cybersecurity technologies do your business currently have in place? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. Mobile security
 - b. Anti-malware software to protect against viruses, spyware, ransomware, etc.
 - c. Web security, such as (D)DoS mitigation services
 - d. E-mail security, spam/phishing protection
 - e. Network security, such as firewalls, Intrusion Prevention Detection Systems
 - f. Data protection and control
 - g. Point-Of-Sale (POS) security
 - h. Software and application security, including vulnerability management
 - i. Hardware and asset management
 - j. Identity and access management
 - k. Physical access controls
 - l. Managing event logs
 - m. (D)DoS Mitigation
 - n. VPN
 - o. Data backup to separate location
 - p. Business does not have any cybersecurity measures in place
 - q. Other [...] **WRITE DOWN ANSWER**
 - r. DK / NA

Awareness Raising

18) Does your company provide employee training to raise information security awareness? **READ CHOICES**

- a. Yes, according to job role and function
- b. Yes, but only where mandated by law/regulations
- c. Others, please specify
- d. No
- e. DK / NA

19) What do you think will help improve your organization's security levels? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**

- a. Senior management commitment
- b. Larger budgets
- c. Increased security department staff numbers
- d. Better employee security awareness
- e. Advanced security technology
- f. Others, please specify
- g. DK / NA

20) What are your organization / enterprise major challenges or barriers to an effective cyber risk management? **READ CHOICES**

- a. Lack of mandate
- b. Lack of resources
- c. Lack of support by executives
- d. Prioritization
- e. Others, please specify
- f. DK / NA

Authentication and Encryption

21) What kinds of encryption strategy does your company employ? **READ CHOICES, MULTIPLE ANSWERS ACCEPTED FOR a-d**

- a. File encryption on laptops
- b. File encryption on smartphones
- c. File encryption on data in the cloud
- d. Other, please specify
- e. My company does not employ any encryption strategy
- f. DK / NA

22) Does your company have a Data Loss Prevention solution in place? **DO NOT READ**

- a. Yes
- b. No
- c. DK / NA

23) Does your company use Two-Factor Authentication? **READ CHOICES**

- a. Yes, deployed to most / all users
- b. Yes, deployed to a minority of users
- c. We are considering / planning to deploy it
- d. No
- e. DK / NA

Supply Chain

- 24) How does your company rate the cybersecurity risk to its supply chain? **READ CHOICES**
The cyber risk imposed by the supply chain partners and vendors is considered to be
- very high
 - high
 - low
 - none
 - DK / NA
- 25) How does your company ensure an adequate and appropriate level of information security over third parties? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- Identifies risks related to third parties as part of information risk assessments
 - Addresses information security issues in a contract
 - Signs confidentiality and/or non-disclosure agreements
 - Imposes corporate security policy and controls on third parties
 - Where permitted, performs background verification checks
 - Controls third-party access to systems and data
 - Regularly monitors and reviews third party services
 - Other [...] **WRITE DOWN ANSWER**
 - DK / NA

Government role

- 26) Do cyber-attacks by nation-state actors affect your business? **DO NOT READ**
- Yes
 - No
- 27) In your experience, Government regulations, laws and industry standards meant to improve managing cyber risks are being:
- very effective
 - somewhat effective
 - not effective
 - even counter-effective sometimes
 - DK / NA

Cybercrime state of affairs

- 28) Do you feel that the COVID-19 pandemic has exacerbated cybercrime against enterprises in [country]? **DO NOT READ**
- yes
 - no
 - not sure
 - DK / NA
- 29) In the past 12 months, have criminals obtained and/or abused payment information from your company or its customers? **DO NOT READ**
- yes
 - no
 - not sure
 - I would rather not say
 - DK / NA
- 30) Over the past 12 months, has your business been affected by deliberate DDoS attacks? **DO NOT READ**

- a. Yes: we couldn't rely on services that we need
 - b. Yes: we couldn't deliver services that we provide
 - c. No
 - d. Not sure
 - e. I would rather not say
 - f. DK / NA
- 31) Do you consider ransomware to be a business risk? **READ CHOICES**
- a. Significant business risk
 - b. Less business risks
 - c. It is overhyped
 - d. Not sure
 - e. DK / NA
- 32) Do you consider business e-mail compromise (CEO Fraud) a business risk? **READ CHOICES**
- a. Significant business risk
 - b. Less business risks
 - c. It is overhyped
 - d. Not sure
 - e. DK / NA
- 33) In the past 12 months, how many times has your company been victim of cybercrime? **READ CHOICES**
- a. never **CONTINUE @ 36**
 - b. 1 time
 - c. 2-5 times
 - d. more than 5 times
 - e. I would rather not say
 - f. DK / NA
- 34) **ASK ONLY FOR 33b-33d.** Over the past 12 months, which types of cybercrime have affected your organization? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. DDoS Attack/Interference
 - b. Hacking attempt
 - c. Phishing Email
 - d. Malware & Trojans
 - e. Spyware / Stealth software
 - f. Fraudulent Emails (e.g. CEO Fraud)
 - g. Helpdesk / Tech scam
 - h. Ransomware
 - i. CEO Fraud (business e-mail compromise)
 - j. Identity Theft
 - k. Other [...] **WRITE DOWN ANSWER**
 - l. I would rather not say
 - l. DK / NA
- 35) **ASK ONLY FOR 34a-34j.** How did the crime(s) affect the organization? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. Website or other online services were taken offline
 - b. Information being leaked in relation to the organization
 - c. Funds were transferred to an unknown bank account
 - d. Payments were made by forced mistake
 - e. Information about IP or staff were leaked online
 - f. Personal data was leaked
 - g. Blackmail attempt was made

- h. DK / NA
- 36) What do you think is the motivation of cyber criminals? **READ CHOICES, RANDOMIZE LIST, MULTIPLE ANSWERS**
- a. Financial gain
 - b. Fraudulent activity
 - c. Defamation
 - d. Disruption
 - e. For fun
 - f. Espionage
 - g. Stately attack
 - h. Other [...] **WRITE DOWN ANSWER**
 - i. **DK / NA**
- 37) Over the past 12 months, how much money has your organization lost due to cybercrime? **READ CHOICES**
- a. none
 - b. < 0.1% of our yearly revenue
 - c. < 1.0% of our yearly revenue
 - d. < 10% of our yearly revenue
 - e. < 100% of our yearly revenue
 - f. more than our yearly revenue
 - g. not sure
 - h. Would rather not say
 - i. DK / NA
- 38) Over the past 12 months, what impact has your organization suffered from cybercrime? **READ CHOICES**
- a. none
 - b. it was a nuisance
 - c. it has impeded our processes
 - d. it has seriously impacted our business
 - e. not sure
 - f. Would rather not say
 - g. DK / NA
- 39) Over the past 12 months, have criminals tried to extort money from your company through cybercrime? **READ CHOICES**
- a. YES, via Ransomware: blocking access to devices
 - b. YES, via Ransomware: encrypting data
 - c. YES, by threatening to publish stolen data
 - d. YES, by asking for money to stop a prolonged DDoS attack
 - e. YES, by exploitation of sensitive personal images
 - f. Other [...] **WRITE DOWN ANSWER**
 - g. NO
 - h. DK / NA
- 40) **ASK ONLY FOR 39a-39f** If so, how much money went to the criminals? **READ CHOICES**
- a. none
 - b. < 0.1% of our yearly revenue
 - c. < 1.0% of our yearly revenue
 - d. < 10% of our yearly revenue
 - e. < 100% of our yearly revenue
 - f. more than our yearly revenue
 - g. not sure

- h. rather not say
 - i. DK / NA
- 41) In the event of a potential or successful attack, would the organization contact Law Enforcement for assistance and/or to investigate or stop the source of the attack? **DO NOT READ**
- a. Yes
 - b. No
- 42) **ASK ONLY FOR 41b** If No, what is the reason(s)? **READ CHOICES**
- a. Don't know who to contact
 - b. Have not been helpful in the past
 - c. Handle the issue internally
 - d. Didn't know this is something they can help with
 - e. DK / NA
- 43) Are there other government or private agencies that you would report any (criminal) cybersecurity incidents to? **READ CHOICES**
- a. Private cybersecurity firm
 - b. Private CERT/CSIRT
 - c. Sectoral CERT/CSIRT
 - d. National CERT/CSIRT
 - e. none
 - f. DK / NA
- 44) Looking at the next 5 years do you expect the cybercrime activities targeting businesses to? **READ CHOICES**
- a. Decrease drastically
 - b. Relatively decrease
 - c. Relatively increase
 - d. Increase drastically
 - e. DK / NA

Organizational Info & Fade out

- 45) How many people does your company employ? **READ CHOICES**
- a. < 10
 - b. 10 – 99
 - c. 99 – 500
 - d. > 500
- 46) Approximately what is your company's yearly revenue? **READ CHOICES**
- a. < 100,000 €
 - b. 100,000 – 1 Mio €
 - c. 1 - 25 Mio €
 - d. > 25 Mio €

Annex 8 – General Population Focus Group Interview Guide

Duration: min. 120-125 min.

1. Warm-up & get together

Duration: 10 min.

- Moderator introduction
 - Discussion rules (no phones, speaking in turns, listening to one another, no good or bad opinions etc.)
 - Participant's presentation: age, city, interests
 - Link to the group theme: we will be talking about online security and online crime

2. Online usage in general

Duration: 25-30 min.

- How often do you spend time online? How long do you usually stay online in one session?
- What do you usually do online?
 - a. Spontaneous
 - b. Prompted
 1. Use of general sites
 - a. Can you please give me some examples of sites that you usually go to?
 - b. What makes you use those platforms?
 - c. How safe do you usually feel when using them? Do you trust those sites?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns?
 - f. Do you take any measures to protect yourself when using those platforms?
 2. Use of Social Media
 - a. Can you please give me some examples of social media that you usually go to? On what SM platform are you signed up?
 - b. What makes you use those platforms?
 - c. For each platform: How safe do you usually feel on this platform? Do you trust it?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns regarding this platform?
 - f. Do you take any measures to protect yourself when using those platforms?
 3. Use of the e-government
 - a. Can you please give me some examples of e-government platforms that you usually use? On what platforms are you signed up?
 - b. What makes you use those platforms?
 - c. For each platform: How safe do you usually feel on these platforms? Do you trust them?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns regarding this platform?
 - f. Do you take any measures to protect yourself when using those platforms?
 4. Use of the e-commerce
 - a. Can you please give me some examples of e-commerce platforms that you usually use? On what platforms are you signed up?
 - b. What makes you use those platforms?
 - c. How safe do you usually feel on those sites? Do you trust those sites?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns?
 - f. Do you take any measures to protect yourself when using those platforms?

3. Cybercrime - Introduction

Duration: 10 min.

- Did anything change in your online routines during the last year?
- Did your feeling of online security change in any way during the last year?
- What do you think about when you first hear the word "cybercrime"? What are the first things that come to mind when you think about cybercrime?
- When have you first heard about cybercrime?
- Where (channel, person, context) have you first heard about cybercrime?

4. Cybercrime & cybersecurity – specific

Duration: 55 min.

- Do you know what cybercrime means?
- What does cybercrime mean to you?
- How would you define a cybercrime?
- What are the main types of cybercrime that you heard of (in your own words)?
- What would you include in this category (activities, places, people etc.)?
- What are the (other) types of crime most resembling cybercrime? In which ways?
- Do you consider this type of crime to be a serious or a less important one? Why?
- What are in your opinion the main causes of this types of crime/cybercrime?
- What are in your opinion the most vulnerable groups/persons to cybercrime? Why?
- What are in your opinion the persons/groups/entities that usually take part in this kind of activities? Why?
- Do you feel vulnerable/ threatened in any way to/by cybercrime? In what way?
- What are the things you generally do to protect yourself from cybercrime?
- If you think you are not doing enough to protect yourself from cybercrime, what are your main reasons for this?

Phishing

- Have you ever heard of *phishing*?
- Do you know what it is?

Phishing is when criminals contact people from a distance: through phone, e-mail, text messages or social networks. There are many names for this, but the principle is the same. The criminals pretend to be someone else and will attempt to trick the recipient into installing malicious software or sending them money or private information.

- Have you or someone around you received any type of phishing message?

If yes: Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?

- Have you or someone around you been a victim of a phishing attempt?

If the person has someone close that was a victim:

- Do you have any details about the context and the outcome?

- Do you think you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from phishing?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Ransomware

- Have you ever heard of *ransomware*?
- Do you know what that is?

Ransomware is an illegal application that criminals use to block access to computers, mobile phones and to the data and photos that they may contain. The criminals will ask the victim for money to release the computer, mobile phone, data or photos.

- Have you or someone around you been a victim of ransomware?

If the person has someone close that was a victim:

- Do you have any details about the context and the outcome?
- Do you think you know enough to protect yourself from this type of cybercrime?
If yes: What are the rules that you follow online to protect yourself from ransomware?
If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Intimidation and abuse

- Have you ever heard of *on-line intimidation and/or abuse*?
- Please give me some examples of what you consider to be forms of online intimidation or abuse
- Have you or anyone that you personally know been insulted, bullied, blackmailed, or intimidated online?
- Have you witnessed any online promotion of hatred, discrimination or violence against people of a certain race, color, descent or origin?
- Do you think the internet is a safe place for minors? What do you think are the most important risks that they face online?
- Do you think you know enough to protect yourself from this type of cybercrime?
If yes: What are the rules that you follow online to protect yourself from intimidation and abuse?
If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Identity theft

- Have you ever heard of *identity theft*?
- Do you know what it is?
Identity theft is a type of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Please read the following carton (participants are provided with the list) and tell me if anything in the list has ever happened to you:

1. become aware that login credentials to a personal account of yours had been exposed online?
2. become aware that a personal account of yours had been accessed, or it was attempted, by anyone you did not mean to access it?
3. become aware that any personal data of yours had been deliberately and illegally exposed online?
4. become aware that any personal data of yours had been abused, or it was attempted?
5. become aware that any of your bank accounts, online payment accounts or credit card details had been exposed online?
6. become aware that any of your bank accounts, online payment accounts or credit card details had been abused by a stranger, or it was attempted?
7. become aware that your personal mobile phone number had been taken over by someone you did not mean to have access to it?
8. found that a phone number or online account of someone you already knew had been taken over, and they were being impersonated when communicating with you?

- Do you think you know enough to protect yourself from this type of cybercrime?
If yes: What are the rules that you follow online to protect yourself from identity theft?
If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Interference (DDoS)

- Have you ever heard of *interference* (also called *DDoS*)?
- Do you know what it is?

Sometimes, online services can be unreachable due to a malfunction. At other times, criminals are blocking access to them.

- Has any of the online services that you rely on been unexpectedly unreachable for a prolonged time?
- How did you react in that situation?
- Do you think you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from interference?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

5. Cybercrime - concerns and expectations

Duration: 10 min.

- From all the types of cybercrimes that we discussed about, what are the ones that occurs most frequently in your country?
- From all the types of cybercrimes that we discussed about, what are the ones that concerns you the most? Why those?
- Should you be victim of a cybercrime, would you report it? Why? Why not?
- Do you think the persons around you would report if any of those crimes happened to them? Why? Why not?
- Where/to whom would you report it?
- Who/what entity/body should deal with cybercrime in your country? Why this one/ones?
- What are your expectations regarding cybercrimes in your country in the next two years? (increase, decrease, stay the same)

6. Quantitative research deep dive (if necessary) - 3 main topics

Duration: 10 min.

- Topic 1
- Topic 2
- Topic 3

Annex 9 – Cybercrime Victims Focus Group Interview Guide

Duration: min. 120-125 min.

7. Warm-up & get together

Duration: 10 min.

- Moderator introduction
 - Discussion rules (no phones, speaking in turns, listening to one another, no good or bad opinions etc.)
 - Participant's presentation: age, city, interests
 - Link to the group theme: we will be talking about online security and online crime

8. Online usage in general

Duration: 25-30 min.

- How often do you spend time online? How long do you usually stay online in one session?
- What do you usually do online?
 - a. Spontaneous
 - b. Prompted
- 5. Use of general sites
 - a. Can you please give me some examples of sites that you usually go to?
 - b. What makes you use those platforms?
 - c. How safe do you usually feel when using them? Do you trust those sites?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns?
 - f. Do you take any measures to protect yourself when using those platforms?
- 6. Use of Social Media
 - a. Can you please give me some examples of social media that you usually go to? On what SM platform are you signed up?
 - b. What makes you use those platforms?
 - c. For each platform: How safe do you usually feel on this platform? Do you trust it?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns regarding this platform?
 - f. Do you take any measures to protect yourself when using those platforms?
- 7. Use of the e-government
 - a. Can you please give me some examples of e-government platforms that you usually use? On what platforms are you signed up?
 - b. What makes you use those platforms?
 - c. For each platform: How safe do you usually feel on these platforms? Do you trust them?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns regarding this platform?
 - f. Do you take any measures to protect yourself when using those platforms?
- 8. Use of the e-commerce
 - a. Can you please give me some examples of e-commerce platforms that you usually use? On what platforms are you signed up?
 - b. What makes you use those platforms?
 - c. How safe do you usually feel on those sites? Do you trust those sites?
 - d. What makes you trust them?
 - e. Are there any aspects that make you question their safety? What are your biggest concerns?
 - f. Do you take any measures to protect yourself when using those platforms?

9. Cybercrime - Introduction

Duration: 10 min.

- Did anything change in your online routines during the last year?
- Did your feeling of online security change in any way during the last year?
- What do you think about when you first hear the word "cybercrime"? What are the first things that come to mind when you think about cybercrime?
- When have you first heard about cybercrime?
- Where (channel, person, context) have you first heard about cybercrime?

10. Cybercrime & cybersecurity – specific

Duration: 55 min.

- Do you know what cybercrime means?
- What does cybercrime mean to you?
- How would you define a cybercrime?
- What are the main types of cybercrime that you heard of (in your own words)?
- What would you include in this category (activities, places, people etc.)?
- What are the (other) types of crime most resembling cybercrime? In which ways?
- Do you consider this type of crime to be a serious or a less important one? Why?
- What are in your opinion the main causes of this types of crime/cybercrime?
- What are in your opinion the most vulnerable groups/persons to cybercrime? Why?
- What are in your opinion the persons/groups/entities that usually take part in this kind of activities? Why?
- Do you feel vulnerable/ threatened in any way to/by cybercrime? In what way?
- What are the things you generally do to protect yourself from cybercrime?
- If you think you are not doing enough to protect yourself from cybercrime, what are your main reasons for this?

Phishing

- Have you ever heard of *phishing*?
- Do you know what it is?

Phishing is when criminals contact people from a distance: through phone, e-mail, text messages or social networks. There are many names for this, but the principle is the same. The criminals pretend to be someone else and will attempt to trick the recipient into installing malicious software or sending them money or private information.

- Have you or someone around you been a victim of a phishing attempt?

If the person has someone close that was a victim: Do you have any details about the context and the outcome?

If the person was the victim of phishing: Please detail, tell me about the context

- How did it happen? Please describe the context
- Who contacted you?
- What did you do? What were the results of your actions?
- Why do you think it happened?
- Did the event affect you in any way? In which way? (personal, emotional, social, relational etc.)
- What impact it has had on you? (low, medium, high)
- Do you think now you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from phishing?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Ransomware

- Have you ever heard of *ransomware*?
- Do you know what that is?

Ransomware is an illegal application that criminals use to block access to computers, mobile phones and to the data and photos that they may contain. The criminals will ask the victim for money to release the computer, mobile phone, data or photos.

- Have you or someone around you been a victim of a ransomware attempt?

If the person has someone close that was a victim: Do you have any details about the context and the outcome?

If the person was the victim of phishing: Please detail, tell me about the context

- How did it happen? Please describe the context
- Who contacted you?
- What did you do? How did you react in that situation? What were the results of your actions?
- Why do you think it happened?
- Did the event affect you in any way? In which way? (personal, emotional, social, relational etc.)
- What impact it has had on you? (low, medium, high)
- Do you think you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from ransomware?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Intimidation and abuse

- Have you ever heard of *on line intimidation and/or abuse*?
- Please give me some examples of what you consider to be forms of online intimidation or abuse
- Have you or anyone that you personally know been insulted, bullied, blackmailed, or intimidated online?
- Have you witnessed any online promotion of hatred, discrimination or violence against people of a certain race, color, descent or origin?
- Do you think the internet is a safe place for minors? What do you think are the most important risks that they face online?

- Have you or someone around you been a victim of an intimidation/abuse attempt?

If the person has someone close that was a victim: Do you have any details about the context and the outcome?

If the person was the victim of intimidation/abuse: Please detail, tell me about the context

- How did it happen? Please describe the context
- Who contacted you?
- What did you do? How did you react in that situation? What were the results of your actions?
- Why do you think it happened?
- Did the event affect you in any way? In which way? (personal, emotional, social, relational etc.)
- What impact it has had on you? (low, medium, high)
- Do you think you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from intimidation and abuse?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Identity theft

- Have you ever heard of *identity theft*?
- Do you know what it is?

Identity theft is a type of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Please read the following carton (participants are provided with the list) and tell me if anything in the list has ever happened to you:

9. become aware that login credentials to a personal account of yours had been exposed online?
10. become aware that a personal account of yours had been accessed, or it was attempted, by anyone you did not mean to access it?
11. become aware that any personal data of yours had been deliberately and illegally exposed online?

12. become aware that any personal data of yours had been abused, or it was attempted?
13. become aware that any of your bank accounts, online payment accounts or credit card details had been exposed online?
14. become aware that any of your bank accounts, online payment accounts or credit card details had been abused by a stranger, or it was attempted?
15. become aware that your personal mobile phone number had been taken over by someone you did not mean to have access to it?
16. found that a phone number or online account of someone you already knew had been taken over, and they were being impersonated when communicating with you?

- Have you or someone around you been a victim of an identity theft attempt?

If the person has someone close that was a victim: Do you have any details about the context and the outcome?

If the person was the victim of identity theft: Please detail, tell me about the context

- How did it happen? Please describe the context
- Who contacted you?
- What did you do? How did you react in that situation? What were the results of your actions?
- Why do you think it happened?
- Did the event affect you in any way? In which way? (personal, emotional, social, relational etc.)
- What impact it has had on you? (low, medium, high)
- Do you think you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from identity theft?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Interference

- Have you ever heard of *interference* (or DDoS)?
- Do you know what it is?

Sometimes, online services can be unreachable due to a malfunction. At other times, criminals are blocking access to them.

- Has any of the online services that you rely on been unexpectedly unreachable for a prolonged time?
- Have you or someone around you been a victim of interference?

If the person has someone close that was a victim: Do you have any details about the context and the outcome?

If the person was the victim of interference: Please detail, tell me about the context

- How did it happen? Please describe the context
- What did you do? How did you react in that situation? What were the results of your actions?
- Why do you think it happened?
- Did the event affect you in any way? In which way? (personal, emotional, social, relational etc.)
- What impact it has had on you? (low, medium, high)
- Do you think now you know enough to protect yourself from this type of cybercrime?

If yes: What are the rules that you follow online to protect yourself from interference?

If no: Are you interested in getting information/training about how to protect yourself from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

11. Cybercrime - concerns and expectations

Duration: 10 min.

- From all the types of cybercrimes that we discussed about, what are the ones that occurs most frequently in your country?
- From all the types of cybercrimes that we discussed about, what are the ones that concerns you the most? Why those?



- Should you be victim of a cybercrime, would you report it? Why? Why not?
- Do you think the persons around you would report if any of those crimes happened to them? Why? Why not?
- Where/to whom would you report it?
- Who/what entity/body should deal with cybercrime in your country? Why this one/ones?
- What are your expectations regarding cybercrimes in your country in the next two years? (increase, decrease, stay the same)

12. Quantitative research deep dive (if necessary) - 3 main topics

Duration: 10 min.

- Topic 1
- Topic 2
- Topic 3

Annex 10 – IT Professionals Focus Group Interview Guide

Duration: min. 120-125 min.

13. Warm-up & get together

Duration: 10 min.

- Moderator introduction
 - Discussion rules (no phones, speaking in turns, listening to one another, no good or bad opinions etc.)
 - Participant's presentation: age, city, interests
 - Link to the group theme: we will be talking about online security and online crime

14. Cybercrime - Introduction

Duration: 10 min.

- What do you think about when you first hear the word "cybercrime"? What are the first things that come to mind when you think about cybercrime?
- When have you first heard about cybercrime?
- Where (channel, person, context) have you first heard about cybercrime?

15. Cybercrime & cybersecurity – general

Duration: 25 min.

- How would you define "cybercrime" (in your own words)?
- What does cybercrime mean to you as a person?
- What does cybercrime mean to you as a professional working in IT security/cybersecurity?
- What are the main types of cybercrime that you know/heard of (in your own words)?
- What would you include in this category (activities, places, people etc.)?
- What are the (other) types of crime most resembling cybercrime? In which ways they resemble cybercrime?
- Do you consider this type of crime to be a serious or a less important one? Why?
- What are in your opinion the main causes of this types of crime/cybercrime?
- What are in your opinion the most vulnerable groups/persons to cybercrime? Why?
 - in general
 - in the company you work for
- What are in your opinion the persons/groups/entities that usually take part in this kind of activities? Why?
- Do you feel vulnerable/ threatened in any way as a person to/by cybercrime? In what way?
- Do you feel vulnerable/ threatened in any way as a professional working in IT security/cybersecurity to/by cybercrime? In what way?
- What are the things you generally do to protect the company you work for/your colleagues from cybercrime?
- If you think you are not doing enough to protect yourself as a person from cybercrime, what are your main reasons for this?
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from cybercrime, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)

16. Cybercrime & cybersecurity – specific

Duration: 55 min.

Phishing

- Have you ever heard of *phishing*?
- Do you know what it is?

Phishing is when criminals contact people from a distance: through phone, e-mail, text messages or social networks. There are many names for this, but the principle is the same. The criminals pretend to

be someone else and will attempt to trick the recipient into installing malicious software or sending them money or private information.

- Have you or anyone in the company you work for received any type of phishing message? Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?
- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from phishing, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Ransomware

- Have you ever heard of *ransomware*?
- Do you know what that is?

Ransomware is an illegal application that criminals use to block access to computers, mobile phones and to the data and photos that they may contain. The criminals will ask the victim for money to release the computer, mobile phone, data or photos.

- Have you or someone in the company you work for received any request of ransomware? Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?
- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from ransomware, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Intimidation and abuse

- Have you ever heard of *on line intimidation and/or abuse*?
- Please give me some examples of what you consider to be forms of online intimidation or abuse
- Have you or anyone in the company you work for been insulted, bullied, blackmailed, or intimidated online?
- Have you witnessed any online promotion of hatred, discrimination or violence against people of a certain race, color, descent or origin in the company you work from?

Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?

- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from intimidation and abuse, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Identity theft

- Have you ever heard of *identity theft*?

- Do you know what it is?

Identity theft is a type of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

- Have you or someone in the company you work for been a victim of identity theft?
Please detail, tell me about the context – when, how, how did you find out, what did you do? What were the results?
- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from identity theft, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Interference/DDoS

- Have you ever heard of *interference or (D)DoS attack*?
- Do you know what it is?

Sometimes, online services can be unreachable due to a malfunction. At other times, criminals are blocking access to them. Technically, a DoS attack overwhelms a system's resources so it cannot respond to server requests. A DDoS attack (with the first D meaning Distributed) is also an attack on a system's resources, but it's launched by a large number of host machines that are infected by malicious software controlled by the attacker.

- Have the company you work for ever been a victim of *DDoS/DoS*?
- Has any of the online services that you rely on been unexpectedly unreachable for a prolonged time?
- Has the company you work for ever been a victim of interference in this sense?

Please detail, tell me about the context – when, how, what happened, what did you do/How did you react in that situation? Have you managed to solve the problem?

- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from interferences like these, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Data breach

- Have you ever heard of a *data breach*?
- Do you know what it is?

A data breach exposes confidential, sensitive or productive information to an unauthorized person/organization.

- Have the company you work for ever been a victim of data breach?

Please detail, tell me about the context – when, how, what happened, what did you do/How did you react in that situation? Did you manage to mitigate the damage?

- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from data breach, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)

- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

CEO fraud/BEC

- Have you ever heard of *CEO fraud* or *Business Email Compromise*?
- Do you know what it is?

CEO fraud is a scam in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR into executing unauthorized wired transfers or sending out confidential information.

- Have the company you work for ever been a victim of CEO fraud?

Please detail, tell me about the context – when, how, what happened, what did you do/How did you react in that situation? Did you manage to mitigate the damage?

- What are you usually doing to protect the company you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for/your colleagues from data breach, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

17. Cybercrime - concerns and expectations

Duration: 10 min.

- From all the types of cybercrimes that we discussed about, what are the ones that occurs most frequently in the company you work for?
- From all the types of cybercrimes that we discussed about, what are the ones that concerns you the most? Why those?
- Should the company you work for be a victim of a cybercrime, would you report it? Why? Why not?
- Where/to whom would you report it?
- Would you report if any of those crimes happened in the company you work for? Why? Why not?
- Do you think the persons in the company you work for would report if any of those crimes happened to them? Why? Why not?
- Where/to whom would they report it?
- Who/what entity/body should deal with cybercrime in your country? Why this one/ones?
- What are your expectations regarding cybercrimes in your country in the next two years? (increase, decrease, stay the same)

18. Quantitative research deep dive (if necessary) - 3 main topics

Duration: 10 min.

- Topic 1
- Topic 2
- Topic 3

Annex 11 – ISP Professionals Focus Group Interview Guide

Duration: min. 120-125 min.

1. Warm-up & get together

Duration: 10 min.

- Moderator introduction
 - Discussion rules (no phones, speaking in turns, listening to one another, no good or bad opinions etc.)
 - Participant's presentation: age, city, interests
 - Link to the group theme: we will be talking about online security and online crime

2. Cybercrime - Introduction

Duration: 10 min.

- What do you think about when you first hear the word "cybercrime"? What are the first things that come to mind when you think about cybercrime?
- When have you first heard about cybercrime?
- Where (channel, person, context) have you first heard about cybercrime?

3. Cybercrime & cybersecurity – general

Duration: 20 min.

- How would you define "cybercrime" (in your own words)?
- What does cybercrime mean to you as a person?
- What does cybercrime mean to you as a professional working in IT security/cybersecurity?
- What are the main types of cybercrime that you know/heard of (in your own words)?
- What would you include in this category (activities, places, people etc.)?
- What are the (other) types of crime most resembling cybercrime? In which ways they resemble cybercrime?
- Do you consider this type of crime to be a serious or a less important one? Why?
- What are in your opinion the main causes of this types of crime/cybercrime?
- What are in your opinion the most vulnerable groups/persons to cybercrime? Why?
 - in general
 - in the company you work for
- What are in your opinion the persons/groups/entities that usually take part in this kind of activities? Why?
- Do you feel vulnerable/ threatened in any way as a professional working in IT security/cybersecurity to/by cybercrime? In what way?
- What are the things you generally do to protect the companies you work for from cybercrime?
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the company you work for from cybercrime, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)

4. Cybercrime & cybersecurity – specific

Duration: 65 min.

- As an ISP, what data do you collect?
- As an ISP, for how long do you retain data?
- As an ISP, how do you assure the proper management and disposal of data?
- How do you delete data?
 - On specific schedule
 - Only on termination of client's contract
- What is a protocol to request deletion of data and information?
- What safeguards and practices do you have in place to vet employees and Contractors who have access to sensitive information?
- As an ISP, do you perform regular penetration testing, vulnerability management, and intrusion prevention?

- Are all network devices located in your ISP secure facilities and under controlled circumstances (ID cards, entry logs)?
- Please describe the policies, procedures, and practices you have in place to provide for the physical security of your data centres and other sites where information will be hosted, accessed, or maintained.
- Are the physical server(s) of your ISP in a secured, locked and monitored environment to prevent unauthorised entry and/or theft?
- Please describe the safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access, or disclosure of information.
- Are backups performed and tested regularly and stored off-site?
- Are software vulnerabilities patched routinely or automatically on all servers?
- As an ISP, do you comply with a security standard such as ISO, the Payment Card Industry Data Security Standards (PCI DSS)?
- How do you block DDOS traffic?

- Which are the most frequent types of cybercrime attacks you have encountered in your activity?
- Have you ever encountered these?
 - social engineering
 - DoS/DDoS
 - reconnaissance attacks
 - malware (ransomware, worms, viruses, botnets)
 - privilege escalation
 - machine compromise
- Please rank them in the order of importance/harm potential

Group exercise: Please choose three types of cybercrime you consider to be most harmful/relevant for your activity (from the ones you mentioned or from the list provided). Please explain your option.

Type 1 (TBD)

- How would you define this type of cybercrime (in your own words)?
- Have any company that you work for been a victim of this type of cybercrime?
Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?
- What are you usually doing to protect the companies you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the companies you work for from this type of cybercrime, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Type 2 (TBD)

- How would you define this type of cybercrime (in your own words)?
- Have you or anyone in the company you work for been a victim of this type of cybercrime?
Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?
- What are you usually doing to protect the companies you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the companies you work for from this type of cybercrime, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)

- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

Type 3 (TBD)

- How would you define this type of cybercrime (in your own words)?
- Have you or anyone in the company you work for been a victim of this type of cybercrime? Please detail, tell me about the context – when, how, who contacted you, what did you do? What were the results?
- What are you usually doing to protect the companies you work for from this type of cybercrime?
- What are the procedures/rules that you follow (describe the process)
- If you think you are not doing enough as a professional working in IT security/cybersecurity to protect the companies you work for from this type of cybercrime, what are your main reasons for this? (barriers) (lack of resources, lack of expertise, lack of support from the management etc.)
- Are you interested in getting information/training about how to protect your company from this type of cybercrime? What information/knowledge do you feel you need? How (what format) and where would you like to receive it?

5. Cybercrime - concerns and expectations

Duration: 10 min.

- From all the types of cybercrimes that you know of, what are the ones that occurs most frequently in the companies you work for?
- From all the types of cybercrimes that you know of, what are the ones that concerns you the most? Why those?
- Should the company you work for be a victim of a cybercrime, would you report it? Why? Why not?
- Where/to whom would you report it?
- Should the one of the companies you work for be a victim of a cybercrime, would you report it? Why? Why not?
- Where/to whom would you report it?
- Do you think the persons in the company you work for would report if any of those crimes happened to them? Why? Why not?
- Where/to whom would they report it?
- Who/what entity/body should deal with cybercrime in your country? Why this one/ones?
- What are your expectations regarding cybercrimes in your country in the next two years? (increase, decrease, stay the same)

Annex 12 – Law Enforcement Focus Group Interview Guide

Focus Group Guide Law enforcement

Duration: min. 110-120 min.

6. Warm-up & get together

Duration: 10 min.

- Moderator introduction
 - Discussion rules (no phones, speaking in turns, listening to one another, no good or bad opinions etc.)
 - Participant's presentation: age, city, interests
 - Link to the group theme: we will be talking about online security and online crime

7. Online usage in general

Duration: 15 min.

- Which online activities you consider to be most dangerous for general population in terms of cyber risk? (spontaneous)
- Please give me some examples and explain why you consider them as dangerous
- Which of the following online activities you consider to be most dangerous for companies in terms of cyber risk? (spontaneous)
- Please give me some examples and explain why you consider them as dangerous

8. Cybercrime - Introduction

Duration: 10 min.

- What do you think about when you first hear the word "cybercrime"? What are the first things that come to mind when you think about cybercrime?
- When have you first heard about cybercrime?
- Where (channel, person, context) have you first heard about cybercrime?
- What does cybercrime mean to you?
- How would you define a cybercrime?
- What would you include in this category (activities, places, people etc.)?
- Have you noticed any changes regarding cybercrime activities during the last year (during Corona crisis)? (increased, decreased, the same)

9. Cybercrime & cybersecurity – general

Duration: 20 min.

- What are the main types of cybercrime that you heard of (in your own words)?
- What are the main types of cybercrime that you usually deal with in your activity?
- What are the (other) types of crime most resembling cybercrime? In which ways?
- Do you consider this type of crime to be a serious or a less important one? Why?
- From your experience, how often a victim of a cybercrime would report it? Why? Why not?
- Where/to whom do they report it?
- Who/what entity/body deal with cybercrime in your country? Why this one/ones?

10. Cybercrime & cybersecurity – specific

Duration: 55 min.

- What are in your opinion the main causes of this types of crime/cybercrime?
- What are in your opinion the most vulnerable groups/persons to cybercrime? Why?
- What are in your opinion the persons/groups/entities that usually take part in this kind of activities? Why?

Attribution (co-ordination & information exchange)

- Do you use any prioritization mechanism for addressing cases? How does it work?

- Are you able to collect the cybercrime information you need? Why (not)?
- Do you use any Big Data repositories? Is cybercrime data treated according to a dedicated body of laws/regulations? (ex. GDPR and/or human rights laws etc.)
- Do you (often) work together with other countries / EU countries? How? Any top countries to mention?
- A lot of the information needs to be collected through international law enforcement mechanisms (e.g. Budapest). Do you feel that those work for you?
- Often, there are dependencies on the private sector. Does information collection from the private sector come into play for you? How?
- Are there information exchanges with the financial industry? Are those effective?
- Are there information exchanges with the telco/ISP industry? Are those effective?
- Are there information exchanges with your national/governmental CERT/CSIRT or other agencies? Are those effective?
- Do you often use specific law enforcement / judicial powers in investigations? Which ones?
- Do you (additionally) use classic criminal intelligence and investigation techniques in the realm of cybercrime?

Disrupting cybercrimes

- Do you (often) technically disrupt/stop cybercrimes that are taking place? How? Under what circumstances are you allowed to?
- Are you allowed to gain access to a suspects' system or device? In what way(s)?

Caring for victims

- Do you notify (potential) victims proactively?
- How do you interact with victims?
- Where/how do victims file their reports?
- Are victims confident that law enforcement can and will do something with their information?
- Do you provide victims with information to improve their own cybersecurity?
- Are you able to successfully combat child abuse material online? How?

Cybercrime prevention

- Is any type of cybercrime prevention program in place in your country?
- Specifically: how do you deal with younger first offenders of cybercrimes?
- How does your country deal with ethical hackers?

Cyber capacity

- Do you use forensic procedures (SOPs) and tools, and what kind?
- Where do they find new talent for cybercrime investigations, is it hard to recruit them and if so, why? Is there a basic level of cybercrime understanding being taught to non-cybercrime police officers?
- Are you able to properly prioritize cybercrime investigations against other types of crime?

11. Cybercrime - concerns and expectations

Duration: 10 min.

- From all the types of cybercrimes that we discussed about, what are the ones that occurs most frequently in your country?
- From all the types of cybercrimes that we discussed about, what are the ones that concerns you the most? Why those?
- Do you consider that law enforcement officers are doing enough at the time to protect the general population and companies from cybercrime?
- If you think that law enforcement officers aren't able to do enough at the time to protect the general population and companies from cybercrime, what are the main reasons for this?
- What are your expectations regarding cybercrimes in your country in the next two years? (increase, decrease, stay the same, shift in nature or scale)