ASSESSMENT REPORT OF MOLDOVA National Computer Incident Response Team (CIRT-MD)

December 2022

ACKNOWLEDGEMENT

The readiness assessment report to establish a national CIRT, Moldova has participated in the online sessions to determine the general situation in terms of cybersecurity.

ITU would like to express its sincere gratitude to the Office of the Deputy Prime Minister on Digitalization and Information Technology & Cyber Security Service (STISC) for the support and assistance offered during the assessment. ITU would also like to acknowledge the contribution made by the local stakeholders during the working sessions.

The recommendations of this report were approved as of September 2022. As the document is released in December 2022, it was updated to reflect the lates cybersecurity developments in the country.

Table of Contents

List of Acronyms and Abbreviations

APT	Advanced Persistent Threats
CAPEX	Capital Expenditure / Capital Expense
CEH	Certified Ethical Hacker
CERT	Community Emergency Response Team
CI	Critical Infrastructure
CIIP	Critical Information Infrastructure Protection
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
CNI	Critical National Infrastructure
CSIRT	Computer Security Incident Response Team
CSRC	Computer Security Resource Center
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
DMZ	Demilitarized Zone
FIRST	Forum of Incident Response and Security Teams
GCFA	GIAC Certified Forensic Analyst
GCIA	GIAC Certified Intrusion Analyst
GCI	Global Cybersecurity Index
GCIv3	Global Cybersecurity Index Version 3
GCIv4	Global Cybersecurity Index Version 4
CIRT-MD	Moldova National CIRT
HR	Human Resources
HW	Hardware
ICT	Information and communications technology
ICT4D	Information and Communication Technologies for Development
ICT Eye	ITU ICT information and provides telecommunication/ICT indicators and statistics, regulatory and policy profiles, and national tariff policies
IHT	Incident Handling Team
IRC	Incident Response Capability
IRT	Incident Response Team
ISP	Internet Service Providers
ITU	International Telecommunications Union
MISP	Malware Information Sharing Platform / Open-Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

MoU	Memorandums of Understanding
OAS	Organization of American States
OLA	Operating Level Agreement
OPEX	Operational Expenditures
PKI	Public Key Infrastructure
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team
SLA	Service Level Agreement
SOP	Standard Operating Procedures
STISC	Information Technology & Cyber Security Service
SW	Software

1 Executive Summary

This document is a report of online sessions carried out by ITU to assess the readiness for an implementation of a national CIRT for Moldova (CIRT-MD).

Before producing this report, the team consulted and interviewed key stakeholders and conducted desk research gathering relevant information and facts to ensure accuracy on the report.

However, there were times when reasonable assumptions were made due to unavailability of information from the stakeholders.

No National Computer Security Incident Response Team capabilities are currently established, which poses a challenge to effectively coordinate incident response and management.

No regulations are in place that require incidents to be reported, there is no mandated authority or protocol to handle such a process.

The government started several coordination mechanisms to identify critical infrastructures and related assets/services. However, there is a need to better disseminate such information to relevant stakeholders.

Communication between the government and CI operators is ad-hoc, therefore coordination is limited. In cases where a coordinated response would be required, neither a cybersecurity operational strategy or plan, nor an official mandate is in place to manage and mitigate cybersecurity incidents.

Similarly, risk management exercises or cyber drills are not conducted at a national level.

The Government of Moldova is currently focused on setting up a Computer Incident Response Team (CIRT), with national responsibility appropriately positioned within the government's institutional and organizational structure.

For the purposes of this report, the proposed National Computer Incident Response Team will hereinafter be referred to as CIRT-MD.

CIRT-MD is the focal point for coordinating the information flow when responding to cyberattacks and will offer remediation of cybersecurity incidents for Moldova. The implementation proposal for the CIRT-MD is divided into three phases. During the first phase, the CIRT-MD will offer its services to sectoral CIRTs/CERTs, government agencies, ministries, law enforcement agencies and regulatory bodies, initially focusing on providing reactive services and some basic levels of proactive services.

It is recommended that the CIRT-MD be an executive authority reporting to The Prime Minister's office.

In the first phase, in the establishment of the national CIRT for Moldova, CIRT-MD would:

a) Develop basic and selected reactive and proactive services.

b) Establish a permanent and appropriate space with recommended IT facilities as well as a secured work area and meeting room.

c) Function as the coordination center for other CERTs/CSIRTs within Moldova once expected capabilities are met;

d) Drive, participate and support the activities of other CERTs/CSIRTs within the Region and globally.

e) Cooperate and collaborate with other international CERTs/CSIRTs for information sharing and coordination.

The readiness assessment shows that Moldova is not immune to cybersecurity issues that are being faced by both developed and developing countries. As more and more services are offered over the Internet, a wider variety of cybersecurity incidents are reported, ranging from distributed denial of service (DDoS) attacks to Internet frauds. The main stumbling blocks to tackle these incidents are the lack of technical skills and organizational mechanisms at a national level.

There are some priority areas that need immediate attention, including to:

a) Provide training prior to starting the CIRT implementation to improve the skill sets and competency of the personnel who will be manning the CIRT-MD in areas of cybersecurity as well as to build their confidence in carrying out their duties;

b) Conduct a training of trainer's program in Cybersecurity in order to increase the pool of experts who could provide capacity building workshops in Cybersecurity at national level;

c) Improve the overall readiness, availability and reliability of ICT infrastructure and services to the public as well as the private sector.

d) Develop applicable policies and regulations for the protection of Critical Information Infrastructure.

e) Develop and implement cybersecurity awareness campaigns for the government and the general public.

f) Develop, implement, and continuously improve cybersecurity legislation.

The development of the above priority areas and the establishment of CIRT-MD can be carried out in parallel.

2 Introduction

2.1 Background

Per the request by the Government of Moldova represented by the Office of the Deputy Prime Minister on Digitalization and Information Technology & Cyber Security Service (STISC), ITU is assisting in the assessment of Moldova's readiness to implement a national Computer Incident Response Team (CIRT). With the support of the Government of Moldova, ITU, conducted online sessions with several stakeholders.

The findings and outcomes of the assessment exercise, stakeholder interviews and additional research serve as the base of this report.

2.2 Mission Objectives

The primary objectives of the project were to assess the current capabilities, resources and readiness of CIRT-MD based on input from various stakeholders. The overall objectives were to:

a) Study and analyze the current cybersecurity status and the needs of Moldova.

b) Provide high-level recommendations to improve the national cybersecurity posture and operations of CIRT-MD; and

c) Include the above content and any other information deemed necessary in a report to be submitted in electronic copy to Moldova.

2.3 Methodology

The assessment project was initiated with a national CIRT assessment questionnaire being distributed to the government's focal point whose main objective was to gain the necessary background information of the ICT and cybersecurity posture of Moldova by the ITU experts.

The offsite research and assessment questionnaire are designed to provide ITU with all the relevant information necessary to ensure a complete analysis of the current posture of the CIRT-MD, as well as a successful realization of the assessment exercise.

The assessment exercise was performed with online breakout sessions, only. The online breakout sessions were developed in the form of discussions and interviews with key stakeholders, which complemented the information gathered in the pre-assessment and desk research that served as the foundation for this assessment report. The capacity building sessions will assist the key stakeholders to gain basic understanding of the challenges of cybersecurity and the roles, responsibilities, as well as functions of a National CIRT.

For additional data and information collection, the experts also performed a review of relevant documents, past reports, policies, strategies, and plans relating to cybersecurity provided by the stakeholders during the interviews and meetings. Lastly, online websites and publications with information on ICT and cybersecurity in Moldova, such as ITU ICT Eye[1], World Bank[2] Indicators, among others, were used to complement the information provided during the assessment exercise.

[1] https://www.itu.int/net4/itu-d/icteye

[2] https://data.worldbank.org/

2.4 ITU CIRT programme

ITU has elaborated a methodology to assist Member States in establishing National CIRTs. It is articulated in four phases from the assessment phase (like the one undertaken in Moldova) to the establishment and improvement.

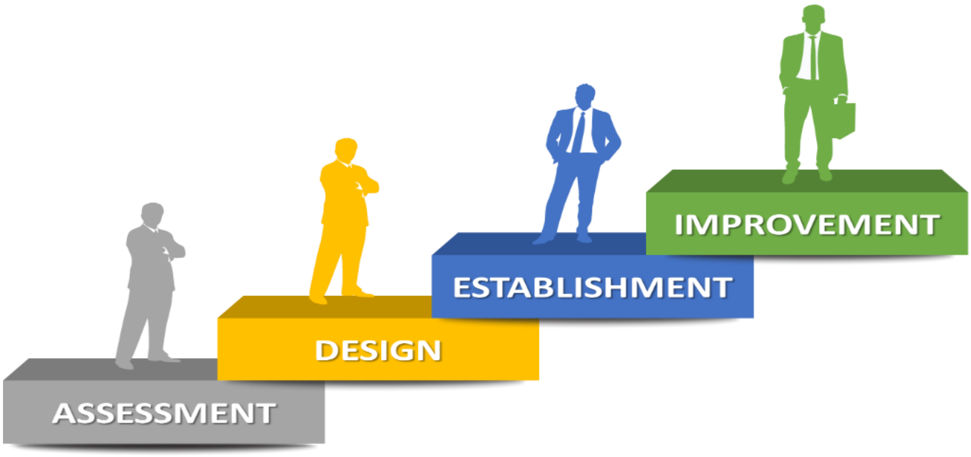


Figure 1: ITU CIRT programme (Source : ITU)

2.5 Design phase

This phase will develop a blueprint of the National CIRT project, with the related implementation processes. The key deliverables of this phase are the CIRT design document and implementation plan.

Table 1: Design phase

Design	
Description	Develop a blueprint of the National CIRT project with the related implementation processes.
Activities	▪ CIRT positioning ▪ Identify CIRT Services ▪ Identify processes and related workflows ▪ Identify policies and procedures ▪ Relationship with constituency and communication strategy ▪ Technology ▪ Premises ▪ HR
Key Deliverables	CIRT design document and implementation plan

2.6 Establishment phase

A basic set of solutions with some technical components such as an incident management system, mailing list, public portal and regularly alerts & advisories on cyber security issues will be needed to operate the CIRT.

Other freely available resources can also be acquired such as membership with the Forum of Incident Response and Security Teams (FIRST). CIRT-MD can become member of FIRST after the CIRT is implemented. Membership with FIRST enables incident response teams to have more effective reactive and proactive reactions to security incidents.

The establishment phase will include the following activities:

Table 2: Establishment phase

Establishment	
Description	Execute the project as agreed with the Member States and based on the outcomes of the Design Service's deliverables.
Activities	▪ Capabilities development ▪ Capabilities deployment and testing ▪ Customization, fine tuning, and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material ▪ Tools

2.7 Improvement phase

The enhancement phase will focus on setting up advanced CIRT services and include the following activities:

Table 3: Improvement phase

Improvement	
Description	Enhance Existing CIRT capabilities and operations
Activities	▪ Environment Analysis ▪ Capabilities deployment and testing ▪ Customization, fine tuning, and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material

3 Cybersecurity Context

Today, the security of a nation is not only restricted to its borders and sovereignty, but it also extends to the protection against new borderless risks and threats. Globalization and the growth of the interconnected global environment through the ICTs and in particular Internet, have brought immense societal benefits but have also opened new avenues for attacks and threats from state's as well as non-state's actors including governments, criminals, terrorists, private companies, and individuals.

The emergence of actors from different locations, with different motives who can employ readily available tools and operate in a global cyber environment makes it incredibly challenging for nation states to employ successful protective measures.

A breakdown of the main cybersecurity actors, their intention and threat types can be found in tables 4 and 5 below.

Governments face a wide range of cybersecurity incidents in their day-to-day reality. There are regular news reports on attacks on vulnerabilities and disruptions to the ICT infrastructure in both the private and public sector. Even more alarming is the increasing number of targeted attacks through Advanced Persistent Threats (APTs) and attacks on critical national infrastructures that could potentially have severe consequences for a nation.

The growing number of cyber incidents act as a clear indicator that it is a challenge for governments around the world to put in place effective and timely response capabilities to cyber threats. The current key trends in cybersecurity include:

a) Consumerization, mobile Internet, and the growth in the number of Internet users are responsible for an incomparable surge in the number of devices connected to the Internet. This development contributes to a more complex management environment and an exponential increase in the number of vulnerable endpoints and users;

b) Digital espionage and cybercrime continue to be the biggest threats for both the public and private sectors;

c) The attacker remains in advantage. Despite of the increased effort from the private industry, governments, and the international community, defenders are still failing to keep up with the complexity, speed, and tools of malicious actors;

d) A significant portion of cybersecurity incidents could have been resolved through simple and easy implementation of preventive measures, highlighting the value of the implementation and auditing of basic security measures as well as cybersecurity awareness and capacity building;

e) Most Internet users and organizations lack the necessary knowledge and skills to protect adequately themselves in the digital environment. As more and more people connect to the Internet, especially in the developing world, this will become an exponentially more serious concern;

f) Malicious actors take advantage of the long response times from governments and private organizations in implementing security measures and deploying security patches. There is a growing need for increased cooperation and information sharing within the international cybersecurity community to develop and deploy more efficient protective measures;

g) The novelty, variety, and complexity of cybersecurity risks and threats require reliable and up-to-date information and situational awareness of the cyber environment;

h) Governments have become increasingly responsible for the coordination of national cybersecurity issues in cooperation with private industry and international actors. National CIRTs have, particularly, become key cybersecurity actors both nationally and internationally.

The goal of all governments should be to achieve a cybersecurity environment where there is no risk of danger or damage to society or citizens coming from the disruption, loss, or abuse of ICTs.

Table 4: Cybersecurity Actors and Intentions

Actor	Intentions	Primary targets	Resources	Prevalence	Visibility
States	Improve position of power	Governments, multinational companies, citizens	High	Medium	Low
Private organizations	Improve information position	Companies	High	Low	Low
Criminals	Monetary gains	Governments, companies, citizens	Average to High	High	Low to Average
Terrorists	Political objectives	Governments, companies, citizens	Few	Low	High
Hacktivists	Ideological objectives	Governments, companies, other groups	Average	Average	High
Script kiddies	Personal interest, to have fun	Governments, companies, citizens, other groups	Low	High	Average
Researchers	Find vulnerabilities	Governments, companies, citizens, other groups	Average	Low	High
Internal actors	Revenge, personal gain	Place of current or former employment	High	Low	Low

Table 5: Cybersecurity Actors and Threats

	Government	Private organizations	Citizens
States	Digital espionage	Digital espionage	Digital espionage
Private organizations		Digital espionage	
Criminals	Disruption as a result of malware, intrusion or spam	Disruption as a result of malware, intrusion or spam	Disruption as a result of malware, intrusion or spam
		Identity fraud	Identity fraud
	Blackmail	Blackmail	Blackmail
	Disruption of online services	Disruption of online services	
Hacktivists	Publication of confidential data	Publication of confidential data	Publication of confidential data
	Disruption of vital infrastructure	The disruption of vital infrastructure	
	Disruption of online services	The disruption of online services	
	Hoaxes	Hoaxes	Hoaxes
Script kiddies	Disruption of online services	Disruption of online services	
Researchers	Publication of confidential data	Publication of confidential data	
Internal actors	Publication of confidential data	Publication of confidential data	
		Blackmail	
Not an actor	Fire, water damage and natural disasters	Fire, water damage and natural disasters	
	Failure of power supply	Failure of power supply	
	Failure and/or absence of hardware and software	Failure and/or absence of hardware and software	

Relevance:

Low Low Low Medium Low High

4 ICT Landscape in Moldova

Moldova's Information and Communication Technology (ICT) sector is one of the most promising emerging economic sectors in the region, representing 7% of GDP in 2019, higher than the EU average of 4%. Moldova's IT sector alone accounts for 3.1% of GDP.[3] Moldova is a small country with few natural resources, but its IT exports has grown 10 times in the last 15 years and the sector offers opportunities for growth and innovation, bolstered by:

- Approximately 2,000 students graduate with a degree in computing or a related field in Moldova every year.
- Moldova's advantages as a subcontracting destination for IT services based on cost, skills, and location.
- Strong growth from SMEs, as Statistics of the National Bureau of Statistics show that Small and Medium-sized enterprises (SMEs) in Moldova's IT sector contribute to Moldova's economy with a notable growth of approximately 15% in 2019 compared to 2018[4].

According to the ITU Measuring Information Society Report 2018, Moldova has a dynamic and competitive telecommunication market, which is characterized by high Internet access speeds, a high level of mobile services accessibility, and technological development. Telecommunication authorities try to apply best practices of market regulation to create a favourable environment for information society development while having minimum intervention from the government.[5]

During the last decade, the Republic of Moldova registered a significant increase in ICT usage and coverage with the rollout on the large scale of fixed and mobile broadband networks. As a result, in 2020, 100% of the country's population is covered by 3G and 99% with 4G/LTE.[6]

According to the National Regulatory Agency for Electronic Communications and Information Technology in Moldova (ANRCETI), fixed broadband access registered a dynamic growth of 7.2% in 2020 in terms of the number of final users compared to 2019, and reached over 719 000 users. Contrarily, the number of mobile internet users decreased by 0.4%, reaching 2 371 108 users.

The number of fixed broadband subscriptions per 100 inhabitants reached a share of 27.2% in 2020, with a 2.2 percentage point increase compared to 2019. The FTTx technology proved to be the most widely used and currently covers 72.3% of fixed broadband subscriptions, registering an increase of 4.9 percentage points. At the same time, xDSL technology ensures

[3] https://neighbourhood-enlargement.ec.europa.eu/system/files/2021-09/moldova_-_sme_fact_sheet_2021.pdf#:~:text=As%20reported%20by%20national%20official,alone%20representing%203.1%25%20of%20GDP.

[4] https://neighbourhood-enlargement.ec.europa.eu/system/files/2021-09/moldova_-_sme_fact_sheet_2021.pdf#:~:text=As%20reported%20by%20national%20official,alone%20representing%203.1%25%20of%20GDP.

[5] ITU Measuring the Information Society Report 2018 - Volume 2, p. 127, retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf

[6] ITU, World Telecommunication/ICT Indicators Database, August 2021, retrieved from https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

19.2% of connections, the coaxial cable connections (DOCSIS) reach 8.2%, and the other technologies cover only 0.3% of connections. [7]

Concerning the mobile broadband market, the number of mobile broadband subscriptions per 100 inhabitants in 2020 was 89.8%, with a 1 percentage point increase compared to 2019. The total number of users accessing mobile Internet via 4G networks increased by 6.8% compared to the end of 2019 and amounted to over 1 600 000. The traffic generated by mobile broadband users via smartphones increased by 47.2% in 2019 to about 52 452 TB and followed the same trend in 2020 when it increased by 55.3% and reached 81 450 TB. [8]

As for the revenue generated in 2020, the fixed broadband Internet market was covered mainly by three operators. In this segment, the biggest share belongs to "Moldtelecom" with 61.1%, which is followed by "Starnet Solutions" with 21%, and "Orange Moldova" with 7.5%. The total share of other fixed Internet access providers was 10.4%, with an increase of only 0.1 percentage points compared to 2019 data.

The mobile broadband market is also divided between three providers. According to the revenue generated in 2020, “Orange Moldova” holds the biggest share of 62%, “Moldcell” has 30%, and “Moldtelecom” share is 8%.[9]

However, the electronic communications market reported in 2020 a decrease of MDL 231.7 mil. (approx. EUR 11.6 million), which is -3.8% compared to 2019, and amounted to approximately MDL 6 billion (approx. EUR 299 million). This was caused by a decrease in sales in almost all the market segments, the only exceptions being fixed and mobile broadband access services. The sales revenue of fixed and mobile broadband services increased compared to 2019 by 1.7% and reached MDL 2.6 billion (approx. EUR 129.6 million). However, the highest revenue growth of 2.8% was recorded in the mobile broadband market.[10] [11]

4.1 Regulatory Landscape

There is strong government support for the ICT sector’s development and promotion. The Government of Moldova has introduced various policies and initiatives to support the ICT sector through education, ICT entrepreneurship, and innovation. In 2016, the “Law on information technology parks[12]” was implemented to create necessary prerequisites to boost the development of the information technology industry, ICT based research, and innovation, educational activities in information technology, as well as create jobs with high added value and attract local and foreign investments. The law set a mechanism for significant reduction of the tax burden by introducing a 7% flat tax on turnover, reduction of bureaucratic barriers,

[7] ANRCETI Report “Anuar statistic dezvoltarea comunicaţiilor electronice în republica moldova, pentru anul 2020”, pp. 4,30, retrieved from https://anrceti.md/files/filefield/Anuar%20statistic_2020.pdf

[8] ANRCETI Report “Anuar statistic dezvoltarea comunicaţiilor electronice în republica moldova, pentru anul 2020”, pp. 4,34, retrieved from https://anrceti.md/files/filefield/Anuar%20statistic_2020.pdf

[9] ANRCETI Report “Anuar statistic dezvoltarea comunicaţiilor electronice în republica moldova, pentru anul 2020”, pp.24, 26, retrieved from https://anrceti.md/files/filefield/Anuar%20statistic_2020.pdf

[10] Using the current exchange rate of the National Bank of Moldova of 20.0639 as of 20.12.2021, retrieved from https://www.bnm.md

[11] ANRCETI Report “Anuar statistic dezvoltarea comunicaţiilor electronice în republica moldova, pentru anul 2020”, pp. 5,23, retrieved from https://anrceti.md/files/filefield/Anuar%20statistic_2020.pdf

[12] Law no. 77 of 21.04.2016 on information technology parks, retrieved from https://moldovaitpark.md/wp-content/uploads/2019/09/Law-77_2016.pdf

and virtual presence in the Park. In 2018, the government developed a "Strategy for the Development of IT Industry and Ecosystem for Digital Innovation for the Years 2018 – 2023"[13] with the objectives to increase competitiveness, diversify the ICT sector and encourage startups. This strategy promotes a competitive IT business environment, human capital in the field of ICT, support for ICT innovations and investment and export support.

Despite its significant progress in ICT, Moldova still faces challenges within its ICT sectors, such as:

- a lack of financing mechanism for IT startups that is regulated and supported by the government.
- insufficiency of IT solutions for the local market;
- local IT companies are focused on outsourcing services, customization, development of solutions of foreign companies, to the detriment of their own IT projects;
- non-resident foreign companies primarily value the added value from the sale of digital products and services, and
- COVID-19 pandemic which has led to delays of local contracts of many IT companies, and it is necessary to support them in order to develop new IT solutions and identify customers in other industries.

In recent years, the government adopted a law on modifications of some normative acts which limit the possibilities of digital interaction between the government, the business community, and consumers. As a result, in 2020, USAID conducted a rapid study on the development of e-commerce in the Republic of Moldova's Structural Reforms Program.

Further in 2013, "The Digital Moldova 2020 strategy"[14] was developed by the Ministry of Economy and Infrastructure and approved by the government in 2013 to promote policies to ensure the ICT sector's sustainable growth. The strategy's vision was to establish by the year 2020 an advanced information society that uses information and communication technology facilities, expanded access to modern ICT infrastructure, rich digital content, and accomplishment information services. The strategy aimed to ease information and communications technology's use more conveniently and encourage systematic development in the next few years, including expanding its use in all areas: public, private, business, and everyday life. The strategy is based on three key pillars, each reflecting the sector's most critical issues:

- Pillar I: Infrastructure and access – the improvement of the connectivity and access to the network".
- "Pillar II: Digital content and electronic services – promoting the generation of digital content and services".
- "Pillar III: Capacities and usage – enhancing literacy and digital skills to enable the innovation and stimulate the usage".

In 2021, "the Moldova Digital Transformation Compact"[15] was jointly developed by ITU and UNDP. As the world recognizes that digitalization is critical to achieving the Sustainable Development Goals, with 2030 fast approaching, Moldova's Transformation Compact acts as

[13] https://eufordigital.eu/library/moldova-strategy-for-the-development-of-the-information-technology-industry-and-the-ecosystem-for-digital-innovation-for-the-years-2018-2023/

[14] https://eufordigital.eu/library/digital-moldova-2020-strategy/

[15] https://www.undp.org/moldova/publications/compact-digital-transformation-moldova

a tool for conveying the vision for digital transformation, supporting leadership and compiling national efforts, donor partnerships and capturing the emerging opportunities as the country enters a new stage.

The Strategy aimed to impact the ICT spread through the public, private, and business areas and envisioned an advanced information society in Moldova by 2020. It was considered a great success with the 95% implementation of the planned actions. As a result, citizens can now benefit from extended access to modern ICT infrastructure, rich digital content, and an extended number of electronic services, as well as from tools and initiatives enhancing digital literacy and technological skills. All these developments raised the ICT sector as one of the engines of the economic growth of the country.[16]

In line with the Strategy objectives, the Broadband Development Program 2018–2020 was approved, and an action plan was adopted for its implementation. The program's overall objective was the development of broadband electronic communication networks, which provide greater data transfer capacity. In order to promote the efficient management of radio spectrum resources and thus ensure the continued development of public broadband electronic communication networks and services, the Radio Spectrum Management Program 2013–2020 was also created.

In 2020, another document adopted to complete the country's legal framework was the Radio Spectrum Management Program 2021-2025, which was developed with the support of ITU. It aims to ensure the radio spectrum resources for the continued development of ICTs in the Republic of Moldova and sets out recommendations for spectrum allocations over the next five years.[17]

From a wider regulatory standpoint, the Republic of Moldova currently scores 91 in the ITU ICT Regulatory Tracker[18]. The ITU Tracker pinpoints the changes taking place in the ICT regulatory environment. It facilitates benchmarking and the identification of trends and gaps in ICT legal and regulatory frameworks, and allows decision-makers to make the case for further regulatory reform towards achieving a vibrant and inclusive ICT sector.

The ICT Regulatory Tracker is composed of 50 indicators grouped into four clusters:

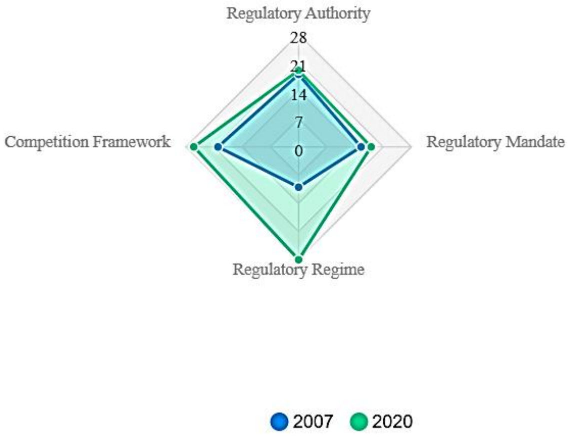
- Regulatory authority (focusing on the functioning of the separate regulator): Moldova scores 19 out of 20;
- Regulatory mandates (who regulates what): Moldova scores 18 out of 22;
- Regulatory regime (what regulation exists in major areas): Moldova scores 28 out of 30;
- Competition framework for the ICT sector (level of competition in the main market segments): Moldova scores 26 out of 28.

[16] https://mei.gov.md/sites/default/files/raport_de_evaluare_moldova_digitala_2020.semnat.pdf?fbclid=IwAR3Ei7fhzkxuWCH9UotCqF3lQx_jUbBzgEwjYbUJkhRZDNKozwXNnEUnSxQ

[17] ITU Collaborative Regulation Case Study for the Republic of Moldova: The Journey to G5 Regulation and Digital Transformation, pp. 12-13, retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2021/National%20Workshop%20for%20Moldova/Moldova_final%20draft_%28clean%29.pdf

[18] https://app.gen5.digital/tracker/country-cards/Moldova

Figure 2 - ICT Regulatory Tracker – Moldova



This benchmark positions Moldova among the group of countries with a Fourth-Generation regulatory regime (G4), that is integrated and led by economic and social policy goals. As the gold standard is currently the Fifth Generation (G5) of regulation, focused on collaboration among different stakeholders in the ICT sector and with other sectors of the economy, there is still room for improvement for the country. [19]

The fundamental shift to the G5 regulation will require Moldova to fine-tune the way regulation is developed and executed. In this context, the ITU report "Collaborative Regulation Case Study for the Republic of Moldova: The Journey to G5 Regulation and Digital Transformation"[20] provides future steps for consideration, grouped into two distinct categories: i) best practice principles of collaborative regulation targeted at improving regulatory maturity; and ii) best practice tools of collaborative regulation that can improve digital market outcomes.

In terms of best practice collaborative regulation principles to improve regulatory maturity, five aspects are envisioned, with recommendations for each of them being provided:

- Regulatory independence and regulatory accountability: function of appointing the Board of "ANRCETI" should be shifted from the Government to the Parliament. Besides, it is important to have another branch of the government reviewing the regulator's decisions in line with established principles of separation of powers.
- Regulatory predictability: putting in place an overarching strategy focused on the development of the digital economy and reviewing the action plan process of ANRCETI could help the Republic of Moldova reach this aim.
- Proactivity: the possibility for ANRCETI to work directly with the Parliament on legislative initiatives could help streamline the process of legal framework improvement in a timely and consistent manner. It is also essential to ensure the participation of all relevant parties from

[19] https://news.itu.int/why-we-need-5th-generation-ict-regulation/

[20] ITU Collaborative Regulation Case Study for the Republic of Moldova: The Journey to G5 Regulation and Digital Transformation, retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2021/National%20Workshop%20for%20Moldova/Moldova_final%20draft_%28clean%29.pdf

the initial stages of legal drafting and complement the existing formal collaboration mechanisms with more flexibility and space for action.

- Collaborative governance: public hearings, high-level roundtables, and expert workshops, hackathons, etc., could strengthen the collaborative culture among stakeholders and help deliver the expected results.
- Regulatory expertise and capacity building: strengthening the capacity of regulators and policymakers to understand and be equipped to deal with the challenges emerging from digitalization is an essential part of the journey towards transformation. Regulatory expertise needs to be developed continuously to integrate new technologies, competencies, and skills and allow for data and evidence-based decision-making.

When it comes to best practice collaborative regulation tools to improve digital market outcomes, two aspects should be taken into consideration:

- Future orientation of policy and regulatory frameworks: Moldova's digital competitiveness can significantly improve through the use of core collaborative regulation tools like pro-competition frameworks for digital transformation, regulatory incentives to innovate, robust and enforceable mechanisms for consumer protection in the digital age.
- Monitoring and evaluation framework and leadership over implementation: introducing appropriate monitoring and evaluation framework gains extra value and may be considered by the Government. From this perspective, establishing a single body with strong coordination powers which is equipped with the necessary tools, could be a guarantee of successful strategy implementation.

As resulted from this research, Moldova's efforts towards a collaborative regulation framework and implementation could benefit from more agile and inclusive mechanisms for collaboration and a new approach to digital markets uplift. In this way, the legal frameworks must be accompanied by a holistic, whole-of-government approach to digitization and sustainable economic development as well as strong leadership in implementation. Also, the collaborative mindset should cut across all levels, sectors, and institutions, and not only be limited to the ICT sector.

4.2 ICT development indicators

The telecommunications market in Moldova is monopolized by the state-owned company Moldtelecom, with a 96 per cent market share in fixed telephony.[21] Moldova has one of the best and most affordable Internet connections in the world, and 5G testing started in. However, it has a lower rate of users with a mobile or internet connection compared to European and CIS countries.

There are more than 20 Internet Service Providers (ISP) in Moldova, with at least 10 fast ISPs. The State-owned Moldtelecom and StarNet are the leading providers in the country, taking up around 88% of the market. The other 12% is shared among other providers, like SunCommunications, Arax Communications, and others. In addition, Moldtelecom offers services to a wide area of the country.

The number of broadband and mobile Internet users has almost doubled. Internet users have reached 76% as of 2017,[22] and most users access services via mobile broadband. And in the

[21] https://www.trade.gov/country-commercial-guides/moldova-information-and-communication-technology

[22] https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx

past ten years, computer ownership in Moldova has increased from 37% in 2010 to 61% in 2020. This increase in ownership has led to a corresponding growth in ICT use.

According to ITU, mobile cellular service is now available in almost all inhabited areas of Moldova, with 100% 3G and 99% 4G coverage as of 2020.

Table 6: ICT indicators per 100 inhabitants-2020 (Source: ITU)

	2010	2020
Mobile-cellular subscriptions per 100 inhabitants	69	85
Fixed-telephone subscriptions per 100 inhabitants	28	25
Active Mobile-broadband subscriptions per 100 inhabitants	3	59
Households with a computer (%)	37%	61%
Households with Internet access at home (%)	27%	65%
Individuals using the Internet (%) (2017)	32%	76%

Source: ITU-Digital Development Dashboard

Figure 3: Fixed-broadband subscriptions per 100 inhabitants (Source: ITU)

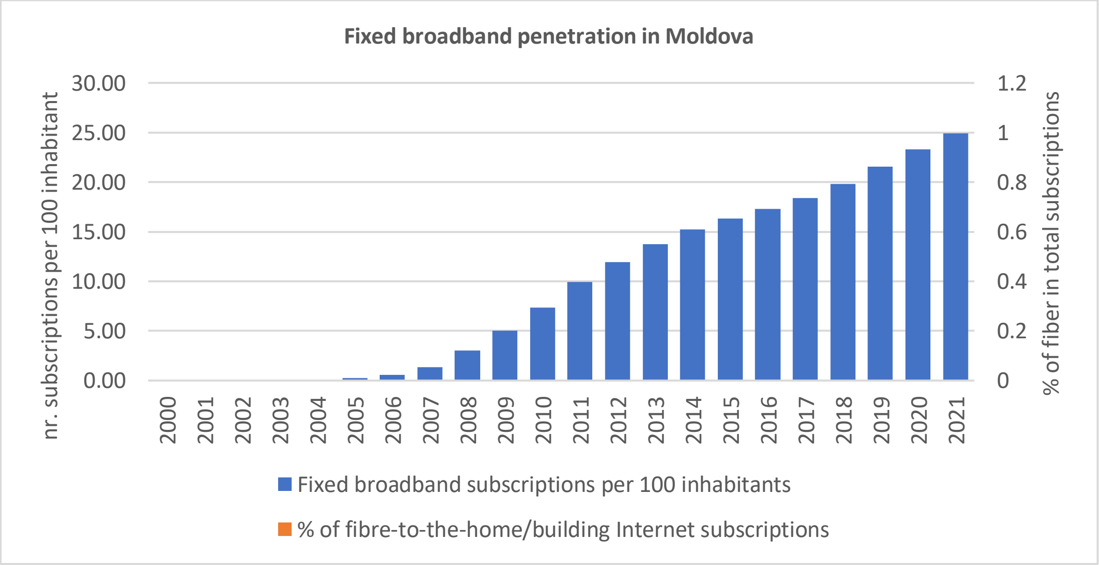
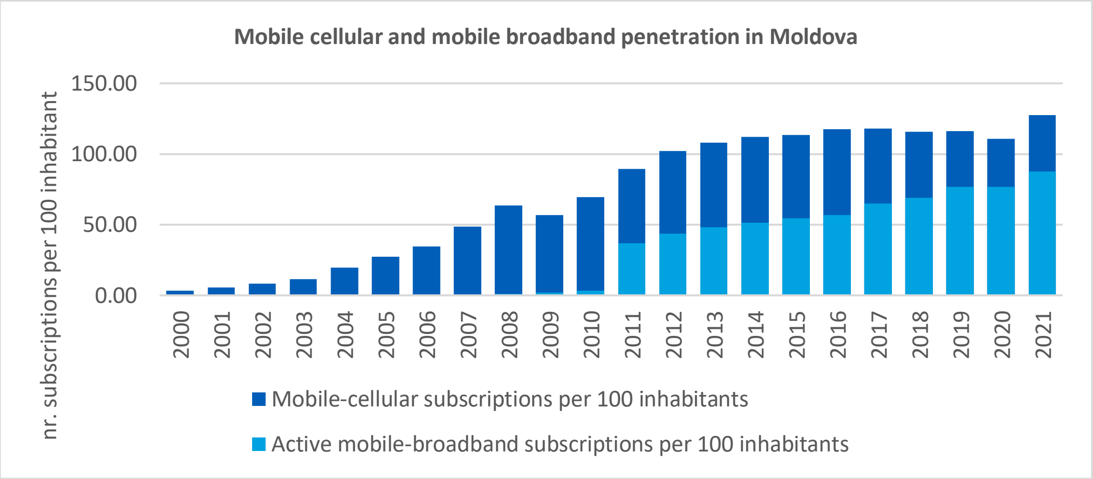


Figure 4: Mobile cellular and mobile broadband in Moldova (Source: ITU)



4.3 Key Observations

ITU recognizes the important work done by the Government of Moldova in transforming the country to an environment favorable to the development of ICT and digital economy.

It is important to continuously adapt to the growing importance of the ICT sector in the development of Moldova, especially in the development of Public Private Partnership investment in ICT, Internet, and E-Government services.

The Government should work towards strengthening the national ICT and cybersecurity sector to reduce the dependency on imported ICT goods and services.

However, it is crucial that decision makers at the governmental level, especially, at the ministerial levels, take into account and allocate sufficient priority to the security, reliability and availability of systems in all ongoing ICT infrastructure projects. The principle of defense in depth should also be adopted by the government in all the projects related to ICT.

Similarly, it is a key for Moldova to continue to develop and sustain sufficient domestic expertise to manage and advance the ICT sector, particularly in terms of ICT security expertise.

The planned expansion of Internet access and E-Government services will also require significant investment by the Government of Moldova in the awareness building and training of citizens and government employees for the safe use of these technologies.

Moldova is at a stage of incorporating new ICT technologies to its Critical National Infrastructure (CNI) and this transition needs systems to be designed to adequate security standards.

An acceptable set of standards for equipment, applications, and security policies should be established to ease ICT management and efficiency.

This process can be supported by CIRT-MD.

5 Cybersecurity landscape in Moldova

5.1 Moldova’s Cybersecurity Commitments measured through the Global Cybersecurity Index

The GCI builds on five pillars, which represent key cybersecurity measures relevant to Member States.

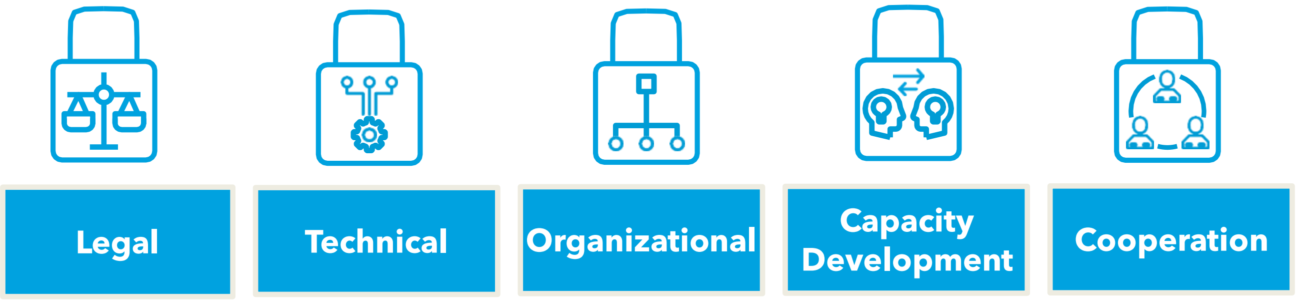


Figure 5: GCI five pillars (ITU)

1. **The legal** environment can be measured based on the existence of legal institutions and effective frameworks dealing with cybersecurity and cybercrime.
2. **The technical** environment can be measured based on the existence of technical institutions and frameworks dealing with cybersecurity endorsed or created by the Member State.
3. **The organizational** structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. Structures such as national agencies need to be established to put the strategy into effect and evaluate the success or failure of the plan.
4. **Capacity Development** is intrinsic to the first three measures (legal, technical, and organizational). Understanding the technology, the risk and the implications can help to develop better legislation, better policies and strategies, and better organization as to the various roles and responsibilities. A capacity building framework for promoting cybersecurity should include awareness-raising exercises and the availability of resources.
5. **Cooperation** enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines, and within private sector operators. It becomes increasingly so at the international level.

The Global Cybersecurity Index (GCI) is designed to drive global cybersecurity awareness, share best practices, drive continuous cybersecurity improvement, and build capacity in ITU Member States.

According to the 2020 ITU Global Cybersecurity Index (GCI), Moldova ranks 33 in the Europe region and 63rd globally.[23] The GCI is a trusted reference that measures the commitment of 194 countries to cybersecurity at a global level while raising awareness of the importance and dimensions of cybersecurity issues and assessing countries' ICT sector resilience and reliability. The GCI assessment methodology analyses how each country addresses cybersecurity issues within their national policies. It is conducted with the help of a questionnaire that addresses the main factors contributing to a country's preparedness in cybersecurity.

Despite its ICT improvements, the performance of Moldova in the Global Cybersecurity Index (GCI) 2020 has declined. This decline can mainly be attributed to removing and adding new

[23] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

questions and changes in the GCI methodology and weightage. However, Moldova has made significant progress since 2015 in measures related to developing and implementing domestic policies, international agreements, and obligations to protect the country's critical information infrastructure.

The GCI assessment shows that the Government of Moldova continues to promote GCI recommendations, notably by enacting relevant legal provisions. For instance, the country has numerous cybersecurity laws and other applicable regulations such as data protection, Child Online Protection, and cybersecurity audit requirements.

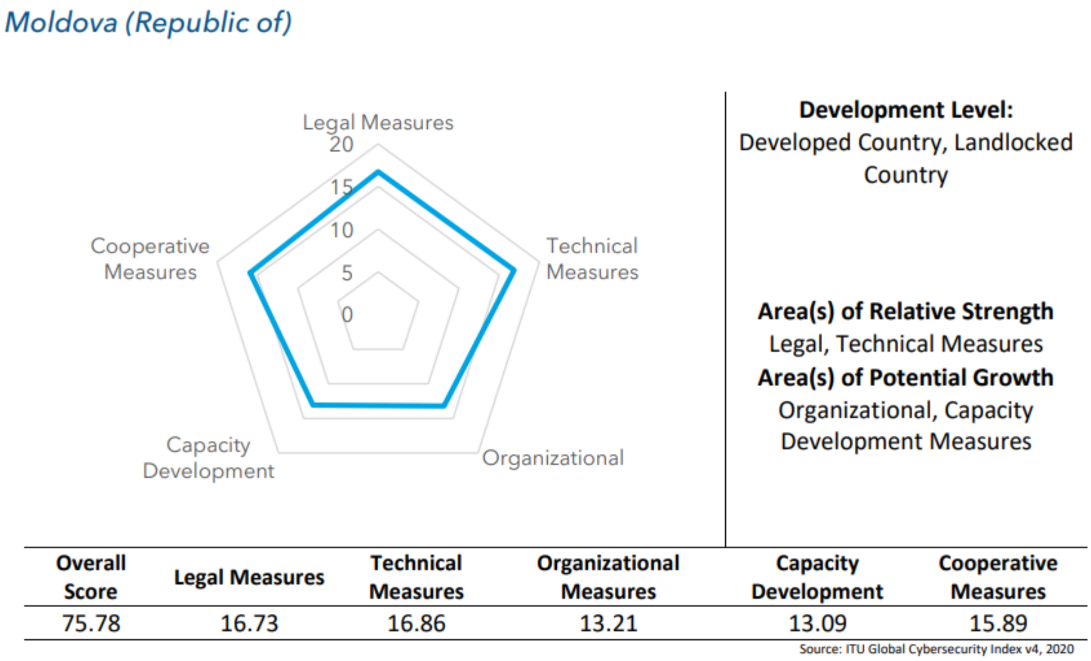
Moldova can improve its legal measures by enacting legislation on:

- online identity and data theft,
- actions related to offences on racist and xenophobic online material and online harassment and abuse against personal dignity/integrity.

Moldova has cybersecurity technical measures in place, such as its “cert.MD[24]” that deal with cyber threats and incidents at the national level. The country also has a national framework for the implementation of cybersecurity standards.

Moldova is increasing its engagement in cybersecurity cooperative measures with other countries and the private sector.

Figure 6: Moldova’s Performance in the GCI 2020



Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.78	16.73	16.86	13.21	13.09	15.89

Source: ITU Global Cybersecurity Index v4, 2020

The radar chart shows that Moldova has room for improvement in certain pillars of the GCI. These include the organizational measures structures such as developing and implementing a clear, unified Child Online Protection national strategy as COP-related elements are

[24] https://stisc-cert.gov.md/index.php/events/workshop-uri/

currently dealt with in different initiatives and not in a harmonized national plan. In addition, adopt measures for evaluating the level of cybersecurity development at the national level.

Capacity development remains an essential area for growth in Moldova.[25] Although there are over 100 schools throughout the country that teach children robotics courses, as part of a nationwide effort led by the government to increase digital literacy and incentives provided for IT parks, the ITU development dashboard shows a lack of ICT standard skills. With over 76% of the population currently online, more active cybersecurity awareness campaigns can help those who have just recently come online gain the necessary skills. It is therefore recommended that Moldova develop awareness campaigns and relevant cybersecurity trainings that cover all online users, including SMEs, the private sector, persons with disabilities, and the elderly; and produce or support professional training courses in cybersecurity, particularly for law enforcement agents, judicial and other legal actors, and SME/private companies.

The government has developed the "TeKwil" initiative[26] – a creation of an excellence centre to enhance education, promote ICT careers, support startups, and establish laboratories, training, and digital education even though the cybersecurity aspect is at its initial stage.

5.2 Cyber threats landscape

Similar to other countries, different types of cyber-attack affect Moldova. They are targeting not only the government entities but also the private sector and population overall.

Though specialized authorities are tracking and monitoring the cyberthreats landscape related to government entities, the holistic understanding of the cyberattacks occurring in the country is missing.

The common types of cybersecurity incidents are related to:

- scams;
- phishing (including smishing and vishing);
- ransomware;
- web defacement;
- denial of service.

Since 2015, the country faced four types of attacks, including DDOS, phishing, brute-force attacks trying to gain access to government information systems, and the hijacking of official web pages.[27] The private sector is targeted in an equal manner by cyberthreats. Large enterprises are equipped with internal policies and tools to be resilient in front of cyber-attacks. Meanwhile, SMEs are struggling to defend themselves and thus represent the most vulnerable part of the private sector. This raises particular concerns as in 2019 SMEs represented about 98.6% of the total number of enterprises [28] , and less than 17% of them have successfully integrated digital technologies in their work. This unveils huge untapped

[25] https://moldovaitpark.md/wp-content/uploads/2021/12/ICT-contents-2021-big-file_final.pdf

[26] https://ict.md/projects/tekwill/

[27] https://balkaninsight.com/2020/10/28/concern-over-moldova-cyber-security-as-election-looms

[28] https://statistica.gov.md/newsview.php?l=ro&idc=168&id=6716

potential, but also highlights an urgent need for SMEs to transform their businesses and adopt cybersecurity protocols.[29]

As an example of cyberattack to this stakeholder group can serve a DDoS attack at the hosting provider AlexHost. The attack power was approximately 900 GB per second with a primary data centre protection level of 500 GB which significantly reduced the ability to restore the centre's performance quickly.[30] Besides, SMEs are frequently a victim of ransomware attacks which result in encryption of their accounting databases.

Citizens are also subject to cyberattacks and the most frequent ones are vishing and smishing. Cybercriminals are successful in these types of attack due to the reduced level of digital culture and cyber hygiene. One of the criminal groups caught in 2021 for theft of money from bank accounts used Viber to contact citizens and present themselves as bank workers. Starting from 2020 and until September 2021 when they've been caught, they made over 40 withdrawals from the bank accounts of several individuals[31].

5.3 Cybersecurity Legal Framework

As part of the efforts to create a comprehensive legal framework, the Government of the Republic of Moldova approved the National Strategy for Information Society Development "Digital Moldova 2020". One of its main objectives was "Enabling the conditions for greater security and trust in digital space". In order to implement this objective, the National Cybersecurity Program 2016-2020 was approved in 2015.

The Program was based on international best practices and implied harmonization with European legislations. It included seven areas of intervention: safe processing, storage and accessing of data, security and integrity of electronic communication networks and services, prevention capabilities and emergency response, prevention and combating cybercrime, strengthening cyber defence capabilities, education and awareness, and international cooperation.[32]

Among the Program implementation results are the approval of the Mandatory Cyber Security Requirements for the public authorities, creation of the Governmental CERT "CERT Gov" and the Military CERT.

However, after the program implementation, with 70% of objectives accomplished, several issues remained unsolved, including the lack of a national CERT, lack of qualified personnel and resources, and insufficient funds dedicated for cybersecurity.[33]

Meanwhile, the National Defence Strategy 2018-2022 and its Action Plan have among its objectives the development of cybersecurity capacities of the central public authorities and

[29] https://www.odimm.md/ro/digitalizarea

[30] https://alexhost.com/data-centre-news/news-about-alexhost-3

[31] https://www.publika.md/s-au-dat-drept-angajati-ai-bancilor-si-au-sustras-circa-un-milion-de-lei-de-pe-cardurile-cetatenilor_3111371.html

[32] ITU Global Cybersecurity Index (GCI) 2018, p.33, retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[33] https://mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf

improving cooperation mechanisms with foreign development partners, including the ones active in the cybersecurity field.

To further advance infrastructure reliability and cybersecurity resilience, Moldova approved the Information Security Strategy 2019-2024 and its Action Plan. It aimed to establish the National CERT, transpose the NIS directive, ensure control and monitoring of the application of minimum cybersecurity requirements, define the national critical infrastructure and the measures needed to protect the critical infrastructure assets, as well as set the framework for counteracting hybrid threats.[34]

In accordance with the Information Security Strategy, the Coordination Council for Ensuring Information Security was established by Government Decision no.467 of 06.07.2022. The Council comprises representatives of legal entities of public and private law and focuses on four areas of activity: cyber, operational, media, and civic-private. When it comes to the actions foreseen to be taken by the Council in the cyber field, it aims to identify and analyze security incidents.[35]

At the moment, the cybersecurity legal framework is comprising:

1. Law no. 241/2007 on electronic communications;
2. Law no. 20/2009 on prevention and combating cybercrime;
3. Law no. 133/2011 on the protection of personal data;
4. Government Decision 1123/2010 on approving the requirements for the personal data protection while processing them in the information systems;
5. Government Decision 1176/2010 on approval of the Regulation on ensuring the secrecy within the public authorities;
6. Government Decision 201/2017 on approval of the minimum cybersecurity requirements for public authorities subordinate to the Government;
7. Government Decision 482/2020 on approval of some measures required for ensuring the cybersecurity of the Government;
8. Government Decision 388/2022 on approval of the Information System Concept of the State Registry of Cyber Security Incidents;
9. Regulation on minimal security requirements for the banking ICT systems, approved by Decision no. 47/2018 of the executive committee of the National Bank of Moldova;
10. Decision no. 60/2019 of the administrative council of the National Regulatory Agency for Electronic Communications and Information Technology on the implementation methods of minimal security and integrity requirements of public telecommunication networks.

5.4 Critical National Information Infrastructure (CNII)

CNII is a term used by governments to describe information assets that are essential for the functioning of a society and economy.

[34] https://mei.gov.md/sites/default/files/strategia_securitatii_informationale_a_republicii_moldova_pentru_anii_2019-2024.pdf

[35] https://gov.md/ro/content/guvernul-creat-consiliul-coordonator-pentru-asigurarea-securitatii-informationale

There is no common and well identified list of Moldova national CNII. There is no standardization of policies or procedures for CNII at the national level.

There is no defined cybersecurity operational strategy for CNII in place to manage and mitigate cybersecurity incidents in case of a coordinated cyberattack on critical infrastructure.

There is no legal framework that clearly defines the national critical infrastructure and measures of its protection. At the moment, there is only a Government Decision no.701/2018 on anti-terrorist protection of critical infrastructure. Besides, measures were taken to protect and fortify the cyber resilience of the telecom operators' networks. The Law on electronic communications no. 241/2007 was amended in 2017 in line with action 2.2 from the National Cybersecurity Program 2016-2020. It aimed at establishing minimum security measures to be taken by providers to ensure the security and integrity of electronic communications networks and/or services and the reporting of incidents with significant impact on them.36 Yet, the existing legal framework is far from being sufficient for ensuring the resilience of the entire national critical infrastructure.

In 2019, a draft law on national critical infrastructure was developed based on Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. However, the work on this law wasn't completed until now.[37]

Recently, a draft law aimed to transpose the NIS Directive was developed by EU4Digital: Cybersecurity East project. This activity was carried out responding to the Government's request, and it is supposed to meet the deadline set by the Information Security Strategy 2019-2024. According to the Strategy, the law should be adopted by the end of 2022. Until then, there is still work to be done for defining the thresholds for identification of the operators of essential services and digital service providers, as well as developing the analysis of the regulatory impact in line with the Law no.100/2017 on the normative acts.

Recommendations

1. The above findings clearly indicate the need for a national CIRT that will act as a focal point in managing incidents and as a coordination center to manage information sharing and information flows so that all relevant parties can report incidents to this central point;
2. CIRT-MD will also provide knowledge of available best practices that can be shared and implemented on the various networks;
3. There is also a clear need for the national CIRT to have an adequate cybersecurity situational awareness system in place (to evolve into a threat intelligence capability) so that the CIRT and its constituency is aware of the types of threats and attacks that are happening both domestically and globally and able to either establish preventive measures or be more reactive in case of breaches;
4. CIRT-MD operational structure should be formally mandated by the government and clearly recognized as empowered entity to deal with incident response and coordination. To this end, according to existing good practices, suitable law or regulation need to be

[36]mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf

[37]https://sis.md/sites/default/files/transparenta/Raport%20realizari%202019%20SSIfinal.pdf

drafted and approved in accordance with prevailing legislative/regulatory national processes and policies;

5. Moldova should recognize the critical and highly interdependent nature of the CNII and aim to develop and establish a comprehensive program and a series of measures that will ensure the effectiveness of cybersecurity controls over vital assets. Moldova needs to ensure that the CNIIs are protected to a level that is proportionate to the risks faced;
6. Outreach programs should be developed to sensitize the public about the dangers associated with cyber threats. Training and education should be conducted to teach users basic steps for dealing with IT security issues;
7. Ensure the security of communication among stakeholders within the redundant communication network.

5.5 Cybersecurity Education and Research

According to the objectives of the National Cybersecurity Program 2016 -2020, the Ministry of Education and Research improved the curriculum in the cybersecurity field. This led to the implementation in 11 higher education institutions, where ICT specialists are trained, of courses that include the information security section. Besides, the Ministry is revising the National Curriculum for schools, which will be updated and completed with content on cybersecurity.

The Technical University of Moldova, under the Information Security study programme, put in place the following courses: Information security basics, Legal framework for information security, Malicious code and antivirus software, Networks administration and security. Besides, courses are being developed in the field of information security for the 2021-2022 academic year, which will be compulsory for all university students.[38] Furthermore, with the support of development partners and private sector companies, several laboratories on cybersecurity-related issues were launched in 2016, 2018, and 2021.

The State University of Moldova implemented the course for bachelor students of the faculty of Mathematics and Computer Science on Cryptography and information security, as well as on Information security management.[39]

Similar to the Technical University, the Academy of Economic Studies of Moldova has established an Information Security study programme. Two courses were generated for the Cybernetics and Economical Informatics specialty dedicated to Administration and security of IT networks and Cryptographic methods for information protection.[40]

[38] Final evaluation report of the National Cyber Security Programme of the Republic of Moldova for the years 2016-2020, p.31, retrieved from https://mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf

[39] https://usm.md/?page_id=515&fbclid=IwAR1AYwLiJzu5kevH__VMHcsyaIj3YgmHj-aOfADWKCc10O6rBdBVKl9KpQU&lang=ru

[40] https://ase.md/programe-licenta

The Academy of Public Administration also created a training module on E-Government, which includes elements of information security, as well as cloud computing technologies and cybersecurity.[41]

For the second cycle degree, the Technical University of Moldova developed two study programmes - Information security and Information security in system and communication networks.[42] The Academy of Economic Studies developed a study programme on the Security of information systems.[43]

The "Stefan cel Mare" Police Academy of the Ministry of Internal Affairs has developed the curriculum on "Cybersecurity and cybercrime". This curriculum led to the development of 7 study programmes on Information security, Cybercrime investigation, Investigating criminal cases of cybercrime, Tactics for documenting and investigating cybercrimes, Legal analysis of cybercrimes, Using EnCase in the handling of evidence electronic, and The use of FTK software in an examination of mobile devices.[44]

Even though there are some high-level university degrees and courses offered in cybersecurity, there is a lack of cybersecurity research in the country.

At the same time, various stakeholders recognize the importance of training in cybersecurity at all levels of education and professional skills development. In this context, ITU has been among the strong supporters of the national efforts through engaging on the yearly basis in "The Moldova Cyber Week" events and capacity-building initiatives. Among them was the first ALERT Cyber Drill 2017 event, which gathered Commonwealth of Independent States (CIS) and European Union (EU) representatives in regional exercise to test, develop and strengthen their cyber-protection skills in Moldova.[45]

Recently, on October 17-18, a Tabletop Exercise (TTX) was organized with the support of the U.S. Department of State, U.S. Civilian Research and Development Foundation. The TTX enhanced the skills of 30 government representatives in testing and evaluating government coordinating structures, processes, and capabilities regarding cyber event response and recovery, and provide a basis for self-identifying and addressing accordingly issues related to cybersecurity incident response capabilities and process gaps.

[41] Final evaluation report of the National Cyber Security Programme of the Republic of Moldova for the years 2016-2020, pp.31-32, retrieved from https://mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf

[42] https://utm.md/procesul-de-studii/masterat/domenii-si-programe-de-masterat

[43] https://tise.ase.md/specialitati-oferite-ciclul-ii-masterat-2

[44] Final evaluation report of the National Cyber Security Programme of the Republic of Moldova for the years 2016-2020, pp.23-24, retrieved from https://mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf

[45] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Moldova_cyberdrill_2017.aspx

Recommendations

1. The most pressing activity is acquiring the right technical expertise into CIRT-MD. This can be achieved by sending the identified candidates to appropriate training and seminars locally (if available) or abroad;
2. Government and stakeholders should conduct a talent search to identify the right people with adequate qualifications to strengthen the operations of CIRT-MD. A Capacity building assessment should also be conducted to identify the right set of courses that the chosen personnel should partake in;
3. Ministries such as the Ministry of Education in coordination with the Deputy Prime Minister on Digitalization must develop cybersecurity specific syllabus that can be made available to local colleges and national universities to produce skilled job ready talented pool of cybersecurity professionals locally;
4. The national CIRT should play a lead role in conducting awareness programs in public organizations and government offices to increase the awareness level;
5. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programs relevant to cybersecurity areas with tertiary students. The research programs can be coupled with rewards such as scholarships or employment opportunities to encourage additional participation;
6. Through partnerships and Memorandums of Understanding (MoUs), the Government can bring in various cybersecurity training providers and make courses accessible in Moldova. Scholarship programs can also be offered to encourage professionals in Moldova to venture into cybersecurity areas;
7. It is strongly recommended that in parallel with the establishment of the National CIRT, the Department of Transformation and Digitization of Moldova conducts a training of trainer's programs in Cybersecurity to increase the pool of experts who would provide capacity building sessions in the Cybersecurity field at national level.

5.6 National Cybersecurity Strategy

In November 2018[46], the Moldovan parliament approved the Information security strategy of the Republic of Moldova for 2019-2024 and the Plan of actions for its implementation Assessment of CIRT-MD, this strategy is based on 4 pillars:

1 Ensuring the security of the cyber information space and investigating cybercrime
2 Ensuring the security of the media information space
3 Strengthening operational capabilities
4 Process efficiency of internal coordination and international cooperation in the field of information security

5.7 Cybersecurity institutional framework

The country is currently lacking a national leading cybersecurity institution. Thus, the legislative and regulatory roles are either divided between different actors or missing.

The legislative role in the cybersecurity field is shared between the following actors:

- Office of the Deputy Prime Minister on Digitalization coordinates the digitalization efforts of authorities to improve the interaction between citizens, entrepreneurs, and

[46] https://rm.coe.int/3-moldova-strategy/168097eceb

the state through modern, convenient, and secure digital tools. It also supervises the activity of the e-Governance Agency, State Service for Information Technology and Cybersecurity, and Public Services Agency.

- Governmental CERT "CERT Gov" within the State Service for Information Technology and Cybersecurity ensures the implementation of the policies on prevention and combating cyber incidents and is a single contact point for reporting the cybersecurity incidents for the public entities subordinate to the Government.
- Ministry of Economy aims to develop and promote policies related to the IT sector and digital economy, with cybersecurity as one of its areas of responsibility.
- Ministry of Infrastructure and Regional Development aims to develop and promote policies directed towards ensuring sustainable growth of the telecommunication sector.
- Ministry of Internal Affairs handles cybercrime-related policies and carries out investigations.
- Security and Intelligence Service is in charge of protection of information systems processing state secret information, investigating large-scale cybercrimes, combating cyber espionage, and ensuring the protection of critical information infrastructure objects.
- Ministry of Defence is responsible for the country's cyber defence and has a functional military CERT within its structure.
- Ministry of Justice pursues cybercrime strategies to ensure an effective criminal justice response to offences against and by computer means.
- Additionally, the Parliament and the Presidential Administration have the right to submit legislative initiative, including cybersecurity-related ones.

The country also has several authorities performing regulatory functions, which are:

- E-Governance Agency monitors the implementation by the public authorities of the cybersecurity audit results regarding minimum cybersecurity requirements, authorizes all public authorities' acquisitions of ICT means, and carries out the cybersecurity audits on ICT infrastructure of the public authorities.
- National Regulatory Agency for Electronic Communications and Information Technology regulates the telecommunication market, ensures the implementation of development strategies, and supervises compliance with the sector legislation.
- National Centre for Personal Data Protection regulates the measures of personal data protection, including of those processed in the information systems.
- Civil Aviation Authority monitors the implementation of aeronautic security measures by aeronautic agents, including the cybersecurity ones.
- National Central Bank regulates and monitors the implementation of minimum security requirements for the banking ICT systems.

The relevant Investigative bodies are the Cybercrime Investigation Directorate under the Ministry of Internal Affairs, the Information Technology and Cybercrime Combating Unit within the Prosecutor's Office, and the Security and Intelligence Service.

Moreover, to coordinate the cybersecurity efforts of all the competent bodies, the Security and Intelligence Service in July 2022[47] established the Coordinating Council for Information Security. This action was undertaken in line with the provisions of Information Security Strategy 2019-2024.

6 General considerations

In general, a Computer Incident Response Team (CIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incidents. Services are usually delivered to a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization, a region or country, a research network, or a paid client.

There are different types of CERT/CSIRT/CIRT or response teams depending on the type of constituency they serve and what type of services they offer.[48] Similarly, there are also several acronyms used to describe teams providing similar types of services such as CSIRC, CSRC, CIRC, CSIRT, IHT, IRC, IRT, SERT and SIRT.[49]

A CIRT primarily focuses on the response to cybersecurity incidents on behalf of one or more constituents by providing:

a) A single point of contact for reporting incidents and incident coordination;

b) Assistance within the constituency and general computing community in preventing and handling computer security incidents;

c) Information and lesson learned to its constituents, other CIRT or response teams, as well as other appropriate organizations and international actors.

6.1 The Role of a National CIRT

A national CIRT responds to computer security or cybersecurity incidents/emergency by providing necessary services to a defined constituency to effectively identify and coordinate threats at the national and regional levels. It also provides information dissemination and acts as the national focal point for matters related to cybersecurity. As of today, there are some 103 to 107 national CIRTs globally.

The fundamental role of a National CIRT, in securing national assets against cyber threats should include:

a. Provide a national mechanism for incident response, coordination, and resolution;

b. Identify and understand current threat landscape and ensure preparedness by adopting appropriate reactive and proactive measures;

[47] https://csometer.info/updates/moldova-new-coordinating-council-information-security-created-government#:~:text=The%20initiative%20is%20part%20of,the%20Action%20Plan%20of%20the

[48] CERT is not an acronym; it is a name and a registered service mark of Carnegie Mellon University. The CERT Coordination Center was the first computer incident response team (CIRT) and although certain CIRT teams have been authorized to use the CERT name by Carnegie Mellon University, the term CIRT is used when referring to general incident response teams.

[49] The definitions are derived from Incident Prevention, Warning, and Response (IPWAR) Manual, USDOE, 205.1-1, Sep 2004 and also Handbook for Computer Security Incident Response Teams (CSIRT), 2nd Edition, April 2003.

c. Always ensure and maintain the safety and societal wellbeing, particularly in times of crisis;
d. Provide appropriate capacity building or training programs to ensure that practitioners are able to handle and communicate incidents in a professional manner;
e. Protect essential services and ensure continuity of Critical National Information Infrastructure;
f. Improve resistance to disruption, breach, damage, and loss;
g. Implement damage control mechanisms for all national ICT assets;
h. Classify sensitive information based on widely adopted information classification system;
i. Implement backup, mitigation, and recovery plans.

6.2 Benefits of Having a National CIRT

The objective of establishing a national CIRT is to establish a trusted focal point of contact within and beyond the national borders for handling cybersecurity matters can provide the following benefits to the nation:

a. A mechanism to identify and manage cyber threats that may have adverse effect on the Government or the nation itself;
b. A mechanism to systematically respond to cybersecurity incidents and take appropriate mitigation actions;
c. The ability for the constituency to recover, quickly and efficiently, from security incidents and minimize loss or theft of information and disruption of services;
d. The utilization of information gained during an incident handling to better prepare for handling of future incidents and better protect systems and data;
e. A mechanism to properly deal with legal issues that may arise during incidents;
f. The encouragement of knowledge exchange within the constituency and the publication of general security best practices and guidance through publications, websites, and other modes of communications;
g. The promotion education, awareness, and training appropriate for a variety of different audiences within the nation;
h. Coordination of cybersecurity and CIRT focal points both within the nation and internationally.

As the national and international coordination centers for cybersecurity issues, national CIRTs play a critical role in building a global cybersecurity environment of trust and achieving a safe cyberspace for all countries.

The national CIRT should be regarded as a key government agency with a critical role similar to the functions of law enforcement, fire emergency services and national defense.

Although a developing country like Moldova faces several fundamental challenges such as the construction of basic infrastructure and similar it is important that the national CIRT is established before a critical attack occurs.

Specifically, CIRT-MD must be seen as a long-term investment and as a building block onto which other cybersecurity projects can be developed.

Figure 7 below elaborates on how ITU visualizes the roles and responsibilities that a national CIRT can play in protecting its country against cyber threats.

It depicts, as well, the relationship between the National CIRT and other relevant initiatives such as national cybersecurity strategies and policies, cyber forensics services, PKI/digital signature initiatives, governance, legislation, critical information infrastructure protection (CIIP) programs, cybersecurity awareness, training and education, research, international cooperation, and security assurance mechanisms.

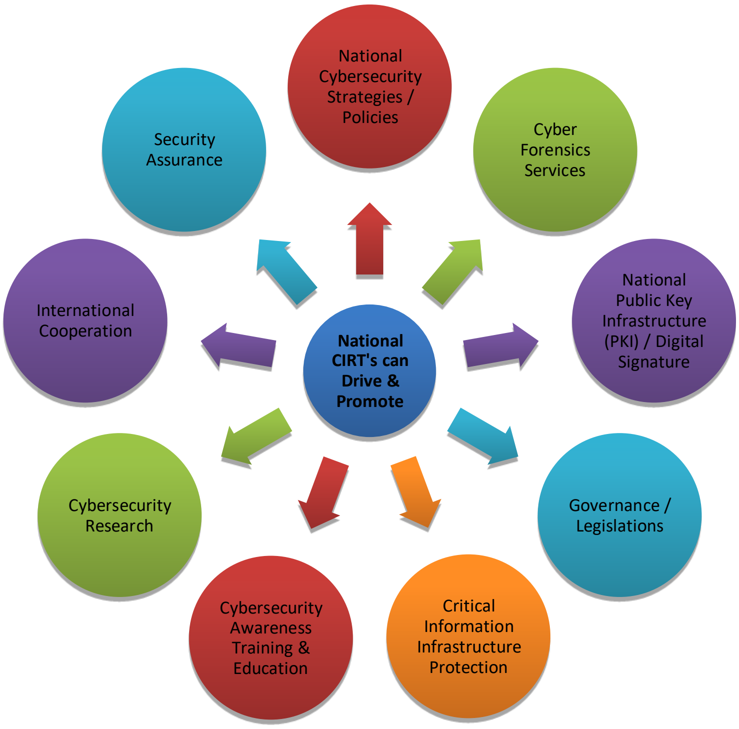

National Cybersecurity Strategies / Policies
Security Assurance
Cyber Forensics Services
International Cooperation
National CIRT's can Drive & Promote
National Public Key Infrastructure (PKI) / Digital Signature
Cybersecurity Research
Governance / Legislations
Cybersecurity Awareness Training & Education
Critical Information Infrastructure Protection

Figure 7: The National CIRT as a Cybersecurity Building Block (Source: ITU)

6.3 CIRT-MD positioning

In General, National CIRTs exist as independent governmental organizations, executive authority under the auspices of a wide range of existing governmental departments or non-governmental organizations. This means that the constituencies served by each National CIRTs are highly variable. For example, some National CIRTs have broad mandates and are responsible for coordinating incident response among all national stakeholders, including the government, network-owner operators, the private sector, and the general public, while others serve some, but not all, of these three.

The authority of the National CIRTs and the actions it is authorized to take differ widely from country to country. Some National CIRTs have regulatory powers, which they can use to compel action from other government agencies and the private sector, while others can act only in an advisory role.

National CIRT are mostly embedded within a government authority or ministry, such as the telecommunications or network information security authority, though some reside in a security or defense ministry. For example:

- Germany's CERT-Bund is part of the Federal Office for Information Security (BHSI), which is subordinate to the Ministry of Interior;
- CERT-Hungary operates as part of the Special Service for National Security, under the Ministry of Interior;

- Mexico's CERT-MX is hosted by the National Commission of Security, which is part for Mexico's Secretariat of the Interior that is concerned with the country's internal security;
- Uganda's CERT-UG is managed by the National Information Technology Authority;
- Tanzania's TZ-CERT functions within the Tanzania Communications Regulatory Authority;
- CERT Australia is part of the Australian government's General Attorney's Department. It is also co-located with cyber security capabilities of other government organizations, including the national signals intelligence and defense organizations, in the Australian national cyber security center;
- Colombia's ColCERT resides within the Colombian Ministry of Defense and houses both the Joint Cyber Command and the Cyber Police Center;
- The Cyber Security Incident Response Team (TTCSIRT) in Trinidad and Tobago reports to the Ministry of National Security;
- CSIRT Chile functions within the Undersecretariat of the Interior and Public Security;
- CSIRT-RD of the Dominican Republic reports to the Ministry of the Presidency and the National Cybersecurity Center.

If embedded in governmental institutions, National CIRTs usually have officially sanctioned authority and may have regulatory powers that they can impose on domestic stakeholders. For example, CERT-Hungary claims that it “may assist in initiating legal proceedings” if necessary, and the Finnish NCSC-FI “can mandate telecommunications providers to take corrective action to support incident response[50].

The National CIRT should be at a level where it can achieve national wide collaboration and information sharing and, when necessary, enforce its mandate. It is important to think about what actions the CIRT will need to take and what type of management support will be required to facilitate those actions during incident handling and response. Identifying such issues may suggest the right reporting or management structure.

Experience shows that the higher up in the government organizational structure the National CIRT is positioned, the better situated it will be to perform its function.

Based on the international good practices mentioned above and the organizational structure of the Government of Moldova and the different mandates of its bodies. It is recommended that the CIRT-MD be an executive authority reporting to The Prime Minister's office.

The assessment exercise showed that there is a need to obtain clarity on some issues that might affect the current set-up of the national CIRT for Moldova; those issues are:

- Delivery mechanisms for existing and new services, institutional relations with the constituency and the relevant national stakeholders;

[50] National CSIRTs and their role in Computer Security Incident Response: Robert Morgus, Isabel Skierka, Mirko Hohmann, And Tim Maurer

https://www.researchgate.net/publication/323358191_National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response

https://www.ncsc.govt.nz/assets/NCSC-Documents/New-Zealand-Security-Incident-Management-Guide-for-Computer-Security-Incident-Response-Teams-CSIRTs.pdf

- Staffing;
- Financing mechanisms; and
- Clear decision on the reporting and overall positioning.

CIRT-MD must be staffed properly with a clear and sustainable financing mechanism that would allow stability and growth.

6.4 CIRT Services

Considering good practices that include a sort of a common approach in structuring the services that a CIRT would provide to its constituency, the service model and the related services will be properly identified during the design mission.

Below is the service structure that would be adopted for CIRT-MD. To be noted that this structure is taken from the current work undertaken by the Forum for Incident and Security Response Team (FIRST)[51], which represent the biggest incident response community globally.

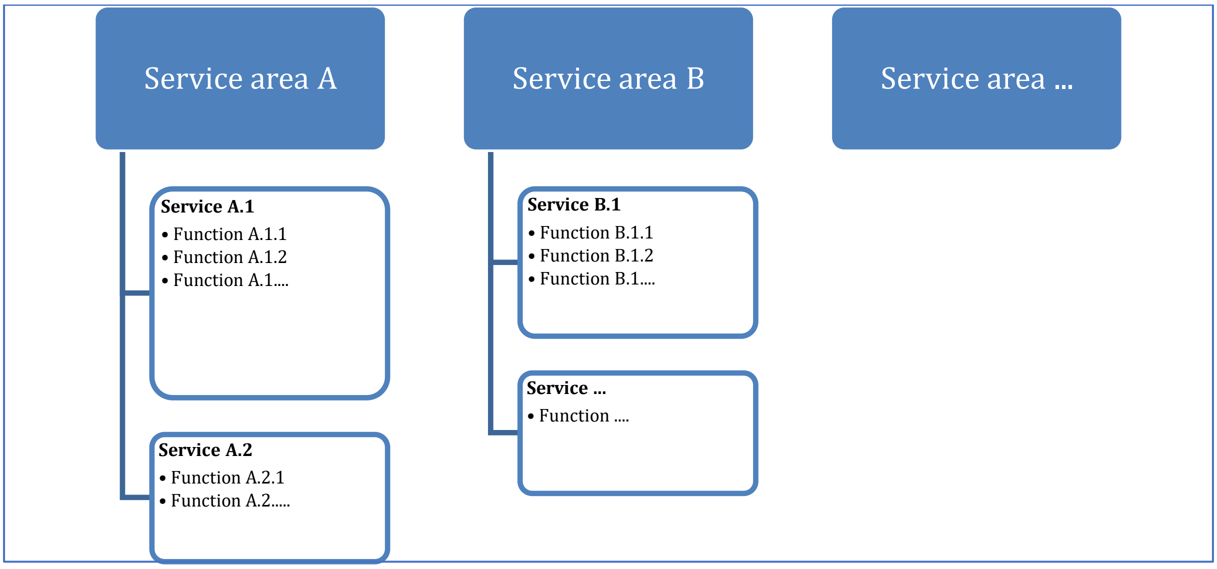


Figure 8: CIRT Service Structure

Service areas represent group of services related to a common aspect. They help to organize the services along a top-level categorization to facilitate understanding. A Service is the set of recognizable, coherent actions towards a specific result on behalf of or for the stakeholder of an incident response team. In addition, functions are specific tasks of a specific service used to implement the service.

6.4.1 *Potential Service model of CIRT-MD*

The following picture highlights the potential set of services that CIRT-MD would be made available. The list of services has been identified are considering the information gathered during the assessment mission.

The final list of services would be agreed during the design phase.

[51]https://www.first.org/education/CIRT_service-framework_v1.1

Table 6: CIRT Potential Services

Service Area	Services
Information Security Event Management	• Monitoring and detection • Event analysis
Information Security Incident Management	• Information security incident report acceptance • Information security incidents analysis • Artefact and forensic evidence analysis • Mitigation and recovery • Information security incident coordination • Crisis management support
Vulnerability Management	• Vulnerability discovery / research • Vulnerability report intake • Vulnerability analysis • Vulnerability coordination • Vulnerability disclosure • Vulnerability response
Situational Awareness	• Data acquisition • Analysis and synthesis • Communication
Knowledge Transfer	• Awareness building • Training and education • Exercises • Technical and policy advisory

A phased approach is recommended for the development and roll-out of the services.

This would ensure the necessary quality in delivering the services, as well as the acquisition of the necessary expertise by CIRT-MD staff.

Also, some of the services might be developed in collaboration with relevant stakeholders. That would generate the establishment of partnerships where staff can be seconded and exchanged between different institutions to enrich the overall knowledge as well as activate knowledge sharing among the community.

6.4.2 Service Parameters

According to international best practices[52] each service will have the following parameters to be properly documented in the service catalogue.

[52] Handbook for Computer Security Incident Response Teams (CIRTs), CMU/SEI-2003-HB-002, Carnegie Mellon Software Engineering Institute

Table 7: Service Parameters

Attribute	Description
Objective	Purpose and nature of the service.
Definition	Description of scope and depth of service.
Service level	The conditions under which the service is available: to whom, when, and how.
Quality assurance	Quality assurance parameters applicable for the service. Includes both setting and limiting of constituency expectations.
Interactions and information Disclosure	The interactions between the CIRT and parties affected by the service, such as the constituency, other teams, and the media. Includes setting information requirements for parties accessing the service and defining the strategy with regard to the disclosure of information (both restricted and public).
Interfaces with other services	Define and specify the information flow exchange points between this service and other CIRT services it interacts with.
Priority	The relative priorities of functions within the service, and of the service versus other CIRT services.

6.5 Processes and Related Workflows

Currently, there are no established processes in place to facilitate notification of incidents, their dissemination or escalation.

It is recommended to elaborate processes aligned as much as possible with existing cybersecurity related law/regulations/directives at the national level, as well as with internationally recognized best practices.

Process engineering should include the development of processes related to the services that CIRT-MD will make available, mainly on incident management and outreach and communication, and the related service level management, which must be agreed with the constituency (the beneficiaries of the services), as well as internal processes to be adopted to properly operate the CIRT, such as IT life cycle, HR, finance, etc.

Also in this case, it is recommended to adopt a phased approach, starting with processes and workflows related to the services - notably incident management, to be followed by the others later.

6.6 Policies and Procedures

There are not any established policies and procedures in place. It is imperative that CIRT-MD be equipped with a set of policies and procedures (including Standard Operating Procedures – SOPs) to ensure cohesion and harmonization in the service delivery. But also provide the constituency indications on how to interact with the CIRT-MD and how to keep their own IT and ICT infrastructures and services as secure as possible.

Typical policies to be build would be, among others:

- Information management (including classification, life cycle, etc.);
- IT security (including network security, usage of devices, etc.);
- Incident handling;
- Acceptable use;
- Data privacy policy;
- Software/hardware usage policy;

- Internet use policy;
- Physical access control policy;
- Social media policy;
- User access policy.

To be noted that a more accurate analysis of the policies needed would be done during the designing phase.

6.7 Interactions with the Constituency and Cooperation

During the sessions, the following constituency for the CIRT-MD has been identified:

- Public sector (all government related institutions, apart from military and intelligence service);
- Private sector (such as ISPs, telecom operators, financial sector, Critical infrastructure providers);
- Academic institutions;
- Judiciary system (including law enforcement);
- General public.

This would imply that CIRT-MD must be able to deliver the agreed set of services to this constituency. As the constituents vary in scope and mandate, it would be recommended to tailor the service delivery according to the specific requirements.

To this end, a service level management process must be put in place to properly identity which specific service is provided to which constituent, and at which condition (SLAs, OLAs).[53]

6.8 Technology and infrastructure

CIRT-MD needs to have a dedicated ICT infrastructure to ensure adequate data separation for its investigations and coordination work.

CIRT-MD should retain control of its own network border firewall, this means that the following assets should remain under the exclusive control of the CERT:

- Network border firewall;
- Primary computing hardware for operational data;
- Backup equipment.

CIRT-MD should control access to its ICT infrastructure either within its secure perimeter or through another secure space within the data center of its building.

A lockable server rack will be required for the machines and the rack must be located in a secure storage room. The network design should be kept as simple as practically possible.

The figure below shows a potential network topology.

[53] ITIL will be used as good practice

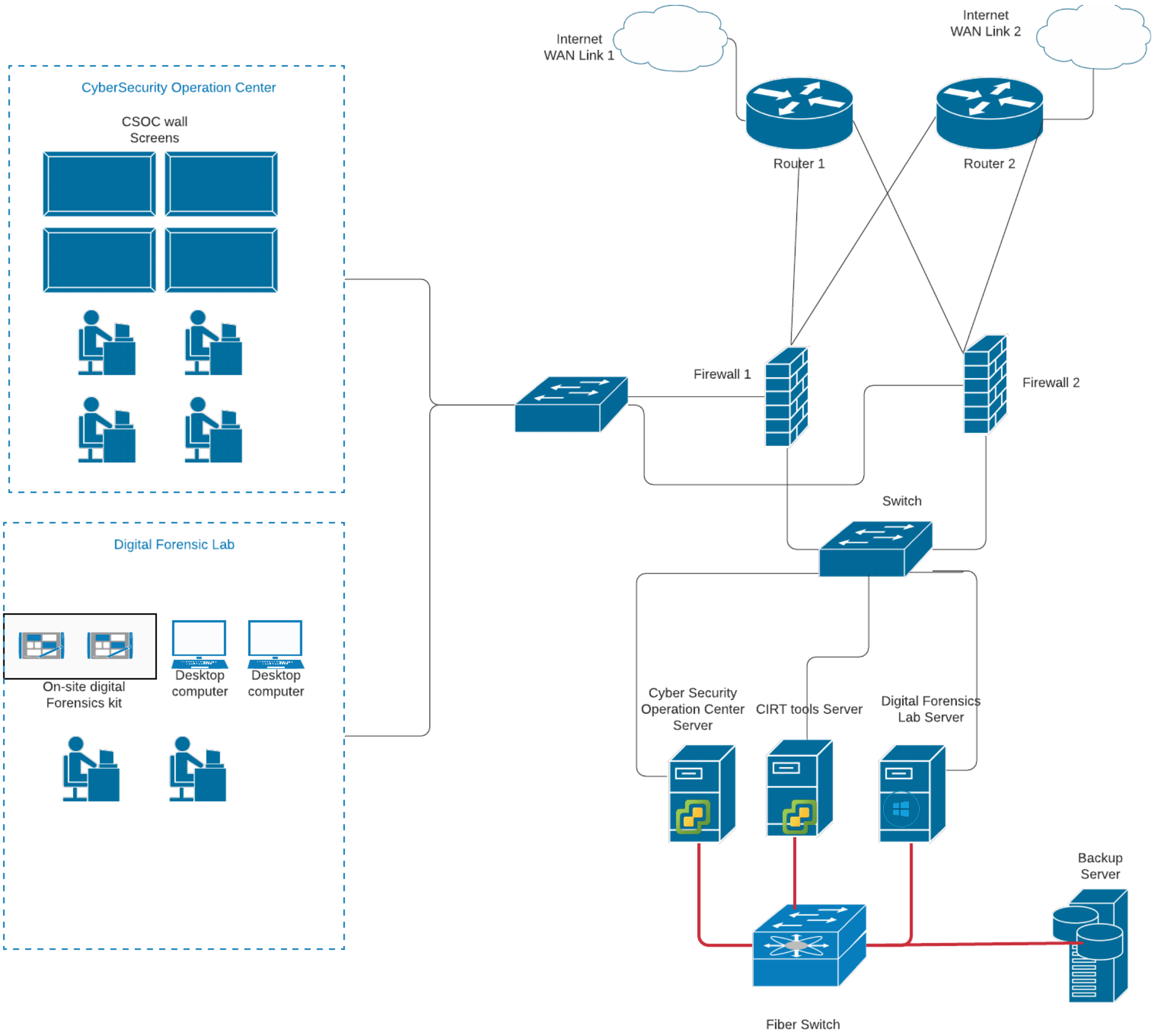


Figure 9: Potential Network Topology

The table below summarizes the list of the essential hardware that is required to operate the CIRT, according to the above network topology. To be noted that the below identified hardware will be sufficient to provide basic CIRT services.

The more mature the CIRT becomes, the more investment in Hardware (HW) and Software (SW) will be needed. The exact list of the equipment and the technical specifications will be finalized during the Design phase.

Table 8: Potential Equipment List

Hardware	Description	Quantity
Router	Connection to the ISP	2
Firewall	DMZ and LAN Firewall	2
Switch	DMZ and LAN Layer 2 Switching	2
CIRT tools Server	A virtualized server that will host 4 VMs: • CIRT WeBHSite • Newsletter management system • Security Incident Response Platform • Threats and Vulnerabilities Tracking tool	1
CyberSecurity Operation Center Server	A virtualized server that will host 3 VMS: • MISP • T-POT • Cyber Threat intelligence	1
Digital Forensics Lab Server	A windows server that will host the investigation tool	1
Storage server	Storage server	1
Fiber Channel switch	Fiber Channel switch	1
Laptop & Desktop Computer	User workstations (incident management, normal office activities	10
Sensors	Honeypot sensors	10
Video Wall Display TV	For visualization and dash boarding	4
On-site digital Forensics kit	On-site digital Forensics kit	1

6.9 Premises

The nature of operations of CIRT-MD makes it necessary for the CIRT premises to have a high level of security. To ensure separation of function, a physical security perimeter will be necessary, and this will entail a separate office space for the CIRT-MD.

The premises should have the following characteristics:

- a separate reception/waiting room for visitors;
- an operations center where the analysts conduct day-to-day activities and other functions;
- an office for the general manager, large enough to accommodate private meetings;
- a path from the reception area to the office that does not transit the operations center;
- a meeting room, ideally with a viewing gallery for the operations center;
- a data storage area for documents and network equipment, which could incorporate the rack space for CIRT-MD infrastructure (see Section 7 on Technology and infrastructure).

The figure below depicts a potential setup for the premises.

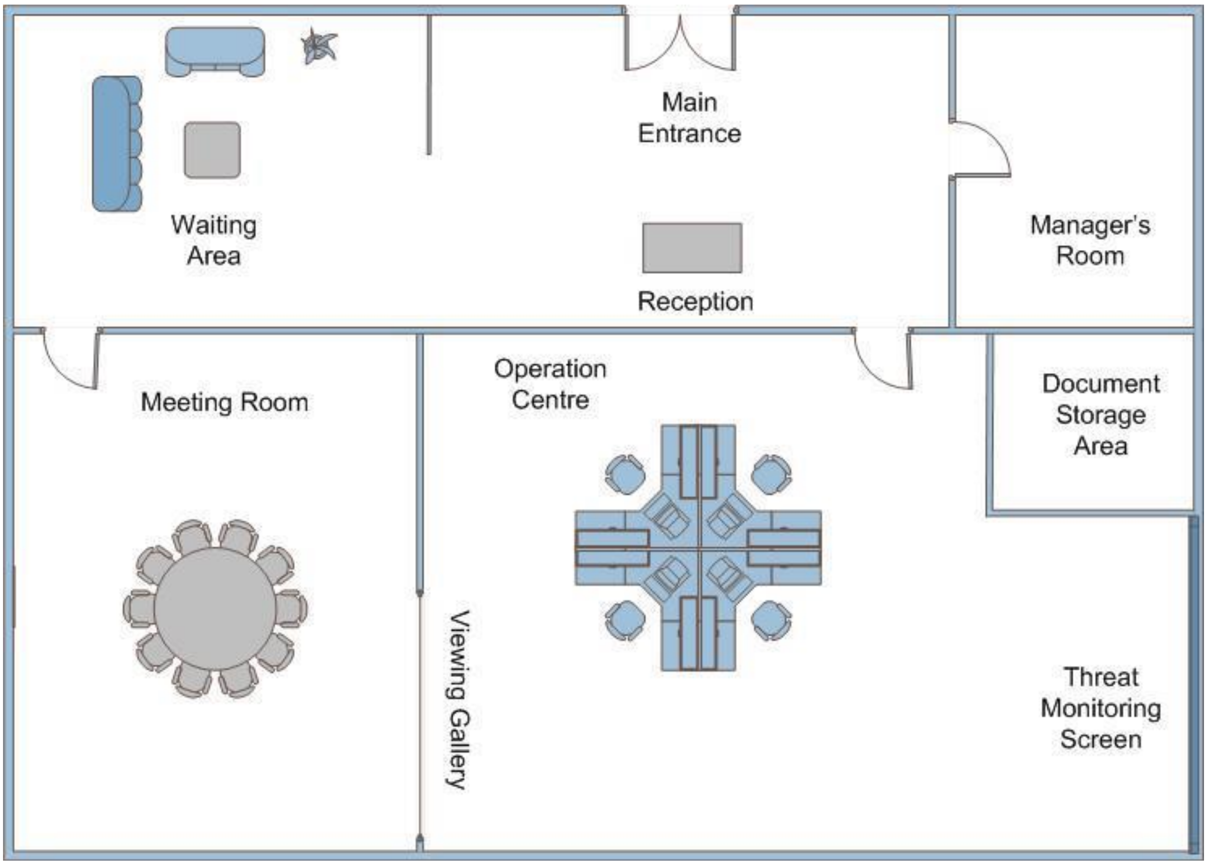


Figure 10: Potential setup of premises

6.10 Human Resources

It is recommended that CIRT-MD be staffed by a minimum of six people: a CIRT Manager, four CIRT analysts.

The CIRT Manager will have the supervisory role to ensure effective operations. The analysts are necessary to ensure that operations may continue in case of absence of one staff.

It is also essential that the staff of the CIRT-MD have opportunities for constant learning and development. Hence, regular trainings should be provided, and the members should be given exposure to international cyber security best practices, events, and conferences.

The exact number of staff has been identified during the design phase. This will vary according to the nature and number of services that the CIRT-MD will make available in the future as well as the magnitude of the constituency (client base) and the operations to be covered.

The below tables are provided as examples of the skillset that might be required.

Table 9: CIRT Manager Skillset

CIRT Manager
Qualifications and Experience • A minimum qualification of a Degree in Information and Communications Technologies, Computer Science or related field backed by a minimum of five (5) years' experience. Candidates with master's degree from a recognized institution of higher learning and a professional certification in security shall have an added advantage. • Professional certification in any related field such as CISSP / CISM/ GCIA / GCFA / CEH is an added advantage. • **1+ year experience of managing a team (desirable)**
Personal Qualities • Good managerial and interpersonal skills. • Self-starter and has high sense of urgency in making deliverables and capable of protecting confidentiality of information. • Able to prioritise tasks and manage time efficiently. • Good personality with ability to work as a team player. • High stress tolerance. • Strong analytical skills. • Willing to travel on short notice.
Technical Competence • An active knowledge of current trends in computer security, software/hardware vulnerabilities • Working knowledge of a broad range of current IT platforms and technologies and at least two operating systems (UNIX and Windows). • Knowledge of risk assessments and cryptographic technologies. • Strong writing skills required for preparation of documents and reports.
Areas of Responsibility and Accountability • To protect national and economic security, the ongoing operations of government, and the ability of critical infrastructures to continue to function. The role will monitor incidents at a national level, identifies incidents that could affect critical infrastructures, warns critical stakeholders about computer security threats, responds to incidents, and helps Critical Information Infrastructure recover from incidents and helps to build organizational CERTs in the public and private sectors. • To provide direction, lead and manage the day to day operations of the unit. • Oversee and prioritize actions during the detection, analysis, and containment of an incident.

• Convey the special requirements of high severity incidents and work directly with the affected network to research the time, location, and details of an incident. • Providing threat intelligence and context for an incident and investigating security incidents. • Development and promote policy and procedures. • Undertake technology watch, the dissemination of information and other tasks when no incidents are ongoing. • Ensures service level commitments. • To plan for the business continuity and disaster recovery of operations. • To advice the Deputy Director on manpower planning and resource allocation. • To coordinate with other department heads / stakeholders on technical matters. • To produce periodic or ad-hoc reports of high quality on the operations of CIRT-MD. • To develop, implement and maintain processes, procedures and guidelines to improve and increase the effectiveness of the operations of CIRT-MD. • To conduct knowledge sharing sessions among other technical personnel on lessons learnt or new findings. • To be aware, comply with and ensure compliance with all CIRT-MD policies, procedures, and guidelines.

Table 10: CIRT Analyst Skillset

CIRT Analyst
Qualifications and Experience • Bachelor's degree in Computer Science/ICT/Engineering – Electronics, Telecommunications, Computer or any relevant area. • Professional certification in any related field such as GCIA/GCFA/ CEH is an added advantage. • Possess at least one (1) year of working experience in relevant field.
Personal Qualities • Strong interpersonal skills. • Self-starter and has high sense of urgency in making deliverables and capable of protecting confidentiality of information. • Able to prioritise tasks and manage time efficiently. • Good personality with ability to work as a team player. • **High stress tolerance.** • **Strong analytical skills.** • Willing to travel on short notice.
Technical Competence • An active knowledge of current trends in computer security, software/hardware vulnerabilities. • Working knowledge of a broad range of current IT platforms and technologies and at least two operating systems (UNIX and Windows). • Knowledge of risk assessments and cryptographic technologies. • Strong writing skills required for preparation of documents and reports.
Areas of Responsibility and Accountability • Reports to CIRT-MD Manager. • To be the support incidents responses in terms of attacks and breaches to information systems in Moldova. • Review current product detections to ensure they are performing to the standard. • Perform tasks to enable detection false positive reduction. • Analyse binary files to determine if they are legitimate or malicious. • Address customer questions and concerns as it relates to detections. • Assist in development and promotion of policy and procedures.

- Develop a representative inventory of critical incidents.
- Develop procedures to follow during an incidence response.
- Recommends updates to the incident response plan.
- Maintains systems for discovering security incidents involving information resources.
- Documents security incidents in a tracking system.
- Further develop incident response program.
- Identify and execute on projects that improve our intrusion detection and incident response capabilities.
- Performs vulnerability assessments and Penetration testing for Critical Information Infrastructure.
- Develops and implements an ongoing risk assessment program targeting CII; recommends mitigation methods.

6.11 Financial considerations

It is necessary to develop a financial plan to ensure long terms sustainability of the CIRT-MD.

Such plan should encompass:

- Capital expenses (CAPEX – one time) to equip CIRT-MD those capabilities and resources that are necessary to operate at peak efficiency (ICT infrastructure, premises, service and product development, among others);
- Operational expenses (OPEX – regular budget) to ensure long term sustainability (salaries, facilities, staff expertise, maintenance of services delivered, among others).

The CIRT-MD might consider cost recovery mechanisms, such as charging in exchange of services delivery that might support financial sustainability while providing added value to the constituency.

This option should be considered only once the services really provide an added value to the constituency.

A detailed financial plan would be elaborated during the design phase.

7 Proposed Action Plan for CIRT-MD

Once the CIRT assessment is completed, ITU proposes to undertake a project aimed to implement the CIRT-MD, using the ITU CIRT programme methodology.

ITU recommends executing a full improvement phase, taking into account the requirements emerged by the design exercise.