REPUBLIC OF BULGARIA

Updated
National Cybersecurity Strategy

"CYBER-RESISTANT BULGARIA 2023"

Council of Ministers

Sofia, 2021

CONTENTS

The Republic of Bulgaria implements a unified national cybersecurity policy, which considers the cybersecurity system as part of the national security protection system. Cybersecurity is defined as a state of society and the state, in which, through the implementation of a complex of measures and actions, cyberspace is protected from threats related to its independent networks and information infrastructure or that may disrupt their operation. Our country actively participates in the formation and implementation of cybersecurity policies within the EU and NATO and strives to achieve cyber resilience of the entire society and state.

A National Cybersecurity Strategy "Cyber-Resilient Bulgaria 2020" was adopted and is being implemented1 a fundamental document for the unified formation, planning, implementation, coordination and control of the policy in the field of cybersecurity, carried out by state institutions in cooperation with business, citizens and their organizations. The National Strategy is synchronized with the EU Cybersecurity Strategy of 2013, and is consistent with the requirements of the EU Directive2 on Network and Information Security. A high degree of

of coherence and continuity between the two documents, relating to the national and European level of security. In implementation of the Directive, the National Strategy was sent to the European Commission and the Member States, and the Commission gave a positive assessment of compliance. The document has also been made available to all NATO partner countries. The National Cybersecurity Strategy expresses the collective commitment and responsibility of all stakeholders and the will of the Government

of the Republic of Bulgaria to guarantee **an open, safe and secure cyberspace.**

The Government Management Program for the period 2017-2021 includes measures to implement key priorities in the field of public order, security and defense. Activities are scheduled to implement the National Cybersecurity Strategy; activities to minimize risks and neutralize threats to national security; to develop capabilities in the field of defense to counter cyberattacks and hybrid impact. During the period 2017-2019, the main regulatory acts were developed and adopted3

which established the legal and regulatory framework for cybersecurity. The law defines the organization and management of the cybersecurity system, establishes the mechanism for coordinated actions at the political and strategic level, specifies the competent authorities for network and information security and their responsibilities, and regulates the general procedure for operational interaction between the relevant institutions and specialized structures. It also regulates the obligations of administrative authorities; persons performing public functions; organizations providing public services; operators of essential services; digital service providers with regard to cybersecurity requirements and cyber incident notification. The Ordinance on minimum requirements for network and information security regulates the minimum measures for managing network and

1 Adopted by Decision of the Council of Ministers No. 583/18.07.2016

2 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

3 Cybersecurity Act, Promulgated in the State Gazette, No. 94 of November 13, 2018; Ordinance on the minimum requirements for network and information security, Promulgated in the State Gazette, No. 59 of July 26, 2019.

information security, protection and resilience measures. Rules have been introduced for carrying out checks for compliance with network and information security requirements; the procedure for maintaining, storing and accessing the register of essential services has been determined, and the forms for incident notifications, the form for summarized statistical information on incidents, and the taxonomy and prioritization in this area have been standardized.

With the adoption of the Cybersecurity Act and related regulatory acts and the institutional building carried out, serious progress was achieved, which gave impetus to the implementation of the measures set out in the Strategy. The horizontal cybersecurity policy is a new area of management and its implementation requires not only significant funds for creating capacities and capabilities of the state, business and society, but also the formation of an entirely new culture of cyber hygiene. In this context, some delay is noted in the implementation of some of the measures envisaged in the National Cybersecurity Strategy.

During the period of implementation of the Strategy, a fourfold increase in the number of reports of computer crimes has been reported. The cyber picture in the country has become more complicated, which is also confirmed by the 45% increase in the number of reports of cyber incidents received over a three-year period, with those with high priority increasing by 29%.4 Cyber incidents with interruption of the services of the Commercial Register in August 2018, as well as the cyber attack against the information system of the National Revenue Agency in July 2019, caused significant public resonance. In the last year, two factors have had a significant impact on the threat picture in cyberspace - the impact of the COVID-19 pandemic and the growing capabilities of cyber threat actors. The significant changes observed in 2019 and 2020 in the cyber picture of threats and risks to cybersecurity at a national and pan-European level (including massive cyberattacks and the connection between cyberattacks, hybrid threats and terrorism, attempts to interfere in democratic processes and directly in elections) require relevant changes to the National Cybersecurity Strategy “Cyber-Resilient Bulgaria 2020”. The update of the Strategy is also necessary in view of the accelerated development of the digital transformation process, as well as for reasons related to the expiration of the Government Management Program. The introduction of changes to the Strategy is consistent with the adopted EU Security Union Strategy5 with a scope of 2020-2025, which, based on an analysis of threats, identifies four interrelated strategic priorities. The first priority is to build capabilities and capacity to ensure a future-proof security environment, and in the

area of cybersecurity, the need for a whole-of-society approach is highlighted, with EU institutions, agencies and bodies, Member States, industry, academia and individuals giving cybersecurity the due priority it deserves. It is noted that the legal framework for the protection and resilience of

4 Statistical data for the period 2018-2020 of NERIX – DAEU 5

COMMUNICATION from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy - **COM(2020) 605 final 24.07.2020**

critical infrastructures6 is not in line with changing risks and adequate measures are needed for their protection and resilience, addressing both physical and cyber security. The next strategic priority of the EU Security Union Strategy is to effectively tackle cybercrime, which is only possible if law enforcement authorities operate in the field of digital investigations with clear rules for investigating and prosecuting crimes and providing the necessary protection to victims. The broadest public awareness should become a key priority so that citizens are aware of the risks and the preventive measures they could take themselves.

could take. This is part of a proactive approach, complementing actions for the full implementation of the current legal framework. The next strategic priority is building a strong European security ecosystem and in particular, cooperation and information exchange.

For the successful implementation of the horizontal policy for digitalization and cybersecurity, new and significant investments are needed. Therefore, in the draft Recovery and Resilience Plan7, the government envisages providing financial resources in the medium term to overcome the slowdown in digitalization in Bulgaria. The improved data transfer environment, as well as digital connectivity and high protection of public institutions, administrations and consumers, will allow for adequate implementation of the measures envisaged under the Cohesion Policy to ensure a high level of cybersecurity. In this regard, when updating the National Cybersecurity Strategy, the opportunities for optimal use of access to financing under the EU Recovery and Resilience Mechanism, as well as funds from European funds and operational programs in the next programming period 2021-2027, were taken into account. This will allow for the initiation and implementation of project packages.

The update of the National Cybersecurity Strategy “Cyber Resilient Bulgaria 2020” is in line with the recently adopted **National Development Program Bulgaria 20308 .** Within the priority “Institutional Framework”, the program states that network and information security is directly related to consumer trust in electronic services, and the safe and widespread use of data-based products and services depends on achieving the highest standards of cybersecurity. The vision and goals of the digital transformation policy of the Republic of Bulgaria for confirm the key interdependence between digital
period 2020-2030 . [9]
technologies and cybersecurity. In this regard, when updating the national cybersecurity strategy, coherence should be achieved with both the goals and the time horizon of the adopted new strategic documents. It is imperative to also define realistic stages for its implementation.

To implement the objectives and measures set out in the Updated Strategy, a Roadmap will be developed, which will be adopted by the Council of Ministers, in implementation

6 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016); Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 7 In coordination procedure with the European Commission, before adoption by the Council of Ministers.

8 Adopted by Protocol No. 67 of the Council of Ministers of 02.12.2020

9 National strategic document “Digital Transformation of Bulgaria for the period 2020-2013”, adopted by Decision of the Council of Ministers No. 493/21.07.2020

of the Cybersecurity Act. Monitoring and evaluation of the implementation and periodic updating of the Strategy and Roadmap is carried out by the Cybersecurity Council.

1. Bulgaria – cybersecurity for digital transformation in a complex and threat-filled environment

1.1 Digital addiction, threats and cybersecurity

Information and communication technologies (ICT) are a key element of the digital transformation in Europe – from smart devices to high-speed internet, mobile applications and research into future and emerging technologies. ICT, together with effectively organised research and education, are also a fundamental factor in building a competitive

knowledge-based economy.

Information and communication technologies are the basis of systems that support the daily activities of state institutions, businesses and citizens, make possible the functioning of the economy in key sectors such as healthcare, energy, finance and transport, ecology and digital infrastructure and last but not least defense, security, crisis management. The state, business and citizens rely on easy access and reliable functioning of communication and information systems and technologies and the Internet environment. In the next decade, an extremely large number of connected digital devices are expected to be present on the territory of the EU, as digitalization and connectivity become essential features of an increasing number of products and services, as well as with new technologies such as the "Internet of Things", big data, etc.

At the end of 2020, nearly 79% of households and over 95% of non-financial enterprises10 in Bulgaria used the internet, with a significant increase in the number of enterprises implementing automated data exchange with external ICT systems. Almost all communication between public administration and business is only electronic. Services to citizens provided via the internet are also growing. Internet connectivity and the speed of information channels are constantly growing - in 2020, Bulgaria ranked 39th in the world out of 221 countries in terms of internet speed, according to the Worldwide Broadband Speed League ranking by Cable.co.uk, with an average speed of 82.42 Mbps for November 2020, it ranks twelfth among the countries with the highest mobile data speed (see:

and with

www.speedtest.net/ global-index). The intensification of efforts to improve and accelerate the deployment of broadband Internet access and the large-scale deployment of digital infrastructure11 will provide new opportunities for remote and cloud services, but also new opportunities for large-scale and malicious use.

10 NSI – study: https://www.nsi.bg/sites/default/files/files/pressreleases/ICT_hh2020_PSRP7D5.pdf___ https://www.nsi.bg/sites/default/files/files/pressreleases/ICT_ent2020_PSRP7D5.pdf

11 National strategic document “Digital Transformation of Bulgaria for the period 2020-2013”, adopted by Decision of the Council of Ministers No. 493/21.07.2020

Digital infrastructures are a critical factor for the management and predictable functioning of resources and systems of national importance, of the modern and innovative economy, of transparent governance, of a free and democratic civil society. Cyberspace provides great opportunities for development, but also leads to a growing and irreversible digital dependence of the main

functions and activities in society. Malicious or unintentional actions can lead to disruption of the operation of management systems and devices related to critical infrastructure and hinder their normal functioning. Threats and risks in cyberspace are difficult to define due to the complexity of determining the source of impact, goals and motives, the rapid escalation of the threat, the difficult to predict development prospects, the complexity and intensity of modern communication and information processes, the dynamics of logical and physical connections and the uncertainty of processes. Identifying, protecting and minimizing these threats and risks are not traditional and require a new culture of interaction between participants in cyberspace.

At the end of the second decade, large-scale cyberattacks rank third in terms of probability of occurrence, after climate change and natural disasters, and cyberdependence is the second factor that will determine the global picture of risks for countries, economies and societies over the next ten years12 .

In 2020, the COVID-19 pandemic accelerated the implementation of ICT for the management and coordination of health authorities, the transition to remote working, the widespread use of teleconferencing as an effective working format, distance learning in an electronic environment. Rapid development is observed in e-commerce, banking payments, insurance. The growth of digitalization and connectivity increases risks for society. The pandemic has made social and economic norms of behavior even more dependent on a secure and reliable cyberspace. The public and private sectors, as well as society as a whole, are equally affected by random cyber incidents or targeted cyber attacks. By their nature, cyberattacks are “asymmetric” – with little effort and investment, huge damage can be caused. Attacks carried out via the Internet are complex, organized and use

a wide range of so-called **“modern persistent threats”13**

, with

a prolonged latent period and the potential to escalate into **a national crisis caused by interference in cyberspace.**

Cyberattacks against **critical infrastructures (CIs)** and vulnerabilities in their management and communication systems have the greatest potential to cause significant damage. A disruption in the operation of common and shared **critical communication and information infrastructure (CII)** has an extraordinary impact on society with unpredictable and potentially catastrophic consequences. The interconnectedness and interdependence in cyberspace allow a security breach or defect in one communication and information system in one sector to have a cascading effect in other sectors with

12 http:/reports.weforum.org/global-risk-2018/global-risks-2018-fractures-fears-and-failures/

13 Advanced Persistent Threats (APT)

serious possible consequences, including the inability to provide vital services. The response to large-scale incidents requires coordinated actions and preventive measures to minimize the possibility of developing into crises, as well as adequate follow-up actions for the timely restoration of normal functioning of systems. A significant part of cyberattacks are malicious actions carried out to obtain financial benefits. Cybercrimes are also committed for the purpose of harassment, fraud, distribution of child pornography, violation of intellectual property rights. Extortion remains widespread, causing

significant damage or causing major harmful consequences to the victims. Counteraction to **cybercrime** is complicated by the increasing number and variety of attacks, the damage and motivation of the people carrying out these attacks.

Sources of organized cyberattacks may be state, military and terrorist organizations, individuals and structures carrying out industrial espionage, cross-border networks and organized criminal groups. A source of a growing threat of a particularly large scale are state-sponsored actors - states with totalitarian regimes and those with an unconsolidated democratic system, with a doctrine of waging information, cyber and hybrid wars. These states, as well as various non-state or terrorist groups, are developing specialized capabilities for **cyberterrorism** and waging **cyberwars** by applying the entire range of methods affecting communication and information systems to violate physical, personal, information and communication security. Among the most serious destructive impacts are those of a hybrid nature. Pulsating, short-term, but very intense attacks on many targets simultaneously, as well as the complexity and scope of the impact can affect all spheres of society and turn into **a hybrid war** against a state or group of states. The threats associated with the trend of spreading and intensifying **radicalization and terrorism** on a global scale are also of a destructive nature, as **cyberspace has become an important arena** and source of risks for the security of citizens, businesses and the state. The Internet is used as the main channel for manipulated information and propaganda, creating psychosis, attracting followers, terrorists and supporting terrorist organizations. The coordinated development of the capacity and capabilities of society by engaging **all stakeholders** guarantees reaching **a new level of maturity in cyberspace** – **cyber resilience.** It is characterized by the ability to meet unexpected, intentional or unintentional threats, to address dynamically changing risks, to adequately respond, control and

recovery.

Cyber resilience requires society to have the capacity and readiness to deal with the “unknown unknowns”, limit the harmful consequences, maximize the preservation and functioning of vital activities and services, and timely recovery. Its achievement requires the security and reliability of the entire **digital ecosystem** - information, organization and processes, technologies, people and facilities, as well as specific requirements for the design and implementation of communication channels, systems and services, their reliable connectivity and operational

compatibility.

1.2 Challenges, threats and risks, opportunities at national level level

Bulgaria is part of the global process of digitalization and increasing digital dependence. **A process of reform of public administration is underway,**
economic and social development **through the implementation of electronic services.** Cybersecurity requirements are essential for the successful implementation of **electronic governance.** The challenges, in addition to those related to technical protection and reliability, are also in building trust and a culture of use, as well as in the timely reporting of incidents and problems. The widespread use of social networks and the Internet in public relations also adds cyber threats of the same importance, scale and speed. The spread of fake news creates

confusion and panic among the population, the modification of faces, speech and gestures of significant political figures, the manipulation of consumer market behavior are a possible element of hybrid warfare and a challenge to which an answer is sought. New technologies and **development trends** provide great opportunities for business, but also lead to new, still insufficiently predictable threats and challenges. With the development of cloud services, Web 4.0 technologies, 5G communications with an emphasis on the protection and control of personal space and data, increasingly rich multimedia forms of communication in social networks, the "Internet of

"safe objects" [14] artificial intelligence systems, the transition to virtual
currencies, quantum technologies, the role of space in cyberspace, etc., risks of the type "modern persistent threats" are expected to increase, which may impact critical resources, systems and services for society in the Republic of Bulgaria.

A specific element in the country is the existence of a wide variety of information systems with different purposes and functionalities, introduced at different periods and at different levels of maturity in terms of interoperability and network and information security (NIS), including communication and information systems operating in critical sectors.

Cybersecurity is a key element of **national security.** Cyberspace is defined as **the fifth area/domain15** for conducting military operations, operations against national interests, territorial integrity, national

security of sovereign states, against the rights and freedoms of citizens16 . The increase in risks and threats in **the geopolitical and strategic security environment,** and in particular in cyberspace, create conditions for increasing vulnerabilities of strategic civil and military communication and information systems and of the command and control systems of forces participating in missions and

14 IoT - Internet of Things - smart devices connected to the Internet /Internet of secure objects/
15 In addition to land, sea, air and space, NATO has defined cyberspace as an area for conducting military operations.

16 NATO - http://www.nato.int/cps/en/natohq/topics_78170.htm
** NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London, 23.05.2019, https://www.nato.int/cps/en/natohq/opinions_166039.htm

operations on and outside the territory of the country. This requires adequate and timely development and acquisition of cyber defense capabilities , as an integral part of the capabilities for protecting the national security management system, related to the defense and guaranteeing the territorial integrity of the Republic of Bulgaria, with the support of international peace and security in an allied and coalition format and the contribution of the Armed Forces to national security in peacetime when managing crises of a non-military nature.

"Cyberattacks can cause damage no less than that caused by conventional methods. A single attack can cause billions of dollars in losses to our economies, bring global companies to a standstill, paralyze our critical infrastructure, undermine democracy, and severely test our military capabilities."

Cyberattacks are becoming increasingly intense, complex and destructive. They range from isolated attempts to high-tech sophisticated attacks. They can be carried out by state and non-state actors. From close proximity or from a great distance. They can affect each and every one of us.

... NATO leaders agreed that a cyberattack could trigger Article 5 of the founding treaty. An attack on one ally is seen as an attack on all. NATO defines cyberspace as a military domain."

*Jens Stoltenberg, NATO Secretary General***

The possibilities for addressing the challenges of the irreversible transfer of the core activities of society, business and government to cyberspace are:

- Increasing the efficiency of technologies at decreasing prices; opportunities for achieving solutions based on an optimal cost-benefit ratio
  realized benefits;
- Virtually unlimited access to a dynamic and global market of cybersecurity products and services – access to technologies related to cryptography, cryptanalysis and intrusion detection;
- Wide access to knowledge, know-how, good practices and solutions in the field of cybersecurity;
- Opportunities arising from EU and NATO membership with a direct impact on the development of coherent policies, appropriate legislation, effectively functioning cooperation in the field of NIS, obtaining assistance when necessary, implementing joint projects, exercises, training and education activities; • Government policy, guaranteeing support and providing large-scale financing of priorities and activities in the field of cybersecurity. Using project management to achieve a cyber-

resilient society, the effectiveness of which would significantly increase with the development and implementation of

a single national cyber resilience programme supporting all e-services. Implementation of projects within the framework of the annual national indicative plans under the Internal Security Fund; planned investments for reforms under the Recovery and Resilience Plan, under the new operational programmes for the next programming period 2021-2027. Priority will be given to projects that are part of the EU's priority value chains. Of particular importance are the opportunities for a joint response in the EU through the Digital Europe and Horizon Europe programmes, as well as programmes in the NATO Communication and Information Organisation.

2. Vision "Cyber-Resilient Bulgaria"

Digital connectivity is the core of digital transformation, and secure cyberspace and trust are key factors for its successful implementation. By 2030, Bulgaria must achieve cyber resilience and build a functioning, reliable and secure digital infrastructure to unlock the full potential of digital technologies for the digital transformation of all key sectors. By 2030, the Republic of Bulgaria will have a **fully** -fledged national cyber resilience ecosystem, integrated into the EU and NATO cybersecurity systems.

2.1. Strategic goal

Digital technologies are transforming the daily lives of citizens and in this process, special attention and care must be paid to cybersecurity. They are of great importance for the transition to the digital economy and society, while simultaneously having a huge impact on the development of the labor market, achieving progress in education and new digital skills, improving competitiveness and innovation, promoting the common good and stimulating the more successful inclusion of citizens. Accelerating digital transformation is an essential element of the response of the EU and its Member States to the economic crisis caused by the COVID-19 pandemic. In this context, a strategic priority in the policy of the Government of the Republic of Bulgaria is the construction of a modern and secure digital infrastructure, as a basis for the digital transformation of the state, business and society. In accordance with the strategies and policies of the European Union and NATO. **The strategic goal** of the government's cybersecurity policy is to achieve **cyber resilience of the entire society and state,** expressed in

effective protection against and adequate response to cyberattacks and cyberincidents, limiting their harmful consequences, ensuring the maximum sustainable functioning of vital activities and services, and timely restoration to normality17 .

To achieve cyber resilience at the national level, it is necessary to go through three consecutive phases, each of which is characterized by reaching a qualitatively new state and **level of maturity** of organizations, the state and society. The three

17 CERT(US) – Resilience Management Model, ISO 27000, NIST standards, etc.

maturity levels - **information security, cybersecurity and cyber resilience18**
can be defined according to two main aspects:

- ensuring the generally accepted "triad" in the field of information security - **Confidentiality-Integrity-Availability (CIA)19;**
- level of knowledge of threats and related risks – a classification of **“known unknowns”,** also used in the field of national security20 . **Figure 1** shows the three levels of knowledge of threats and
  risks and

the corresponding levels of cybersecurity status:

Figure 1. Threat and risk awareness levels and cybersecurity levels

- **"known known" level** – protection and safeguarding of information assets and communication infrastructure from known weaknesses, threats and breaches related to the basic "triad" of **information security;**
- **level “known unknowns”** - alleged complex and combined threats related to information security, ICT, networks and systems, a variety of **modern persistent threats21,** attacks against the reputation of organizations and individuals, disinformation campaigns, and other unpredictable consequences of the mass transfer of activities in cyberspace, breakthroughs in the CIN triad on a particularly large scale (national, regional and global), requiring expanded and systematic application of CIN for all assets in the digital ecosystem - information, technologies and facilities, organization and processes and people, to achieve cybersecurity; • **level “unknown unknowns”** or preparation for the unknown - unexpected threats in cyberspace,

dynamically changing risks and complex impacts with unpredictable consequences that require flexibility

18 Eurocontrol: Manual for National ATM Security Oversight (2012)

19 Confidentiality, Integrity, Availability (CIA)

20 Nassim Taleb, The Black Swan - https://en.wikipedia.org/wiki/Black_swan_theory;

21 Advanced persistent threats (APT)

and resilience of systems, organization and processes, and relevant standards in their development and implementation, **state of cyber resilience.**

To achieve cyber resilience, as the highest level of maturity, systematic, planned and coordinated actions of all stakeholders and clearly defined and phased measures are required in each of **the three phases, with clear leadership and resource provision.**

Phase 1 (initiating): Initiating and achieving basic cybersecurity capacity - **cyber-secure institutions.**

The focus is on achieving a minimum common level of MIS at the level of individual organizations/regulatory entities, building a **National Coordination-Organizational Network for Cybersecurity** with the relevant mechanisms, processes and technical platform, through which information is transferred and operational cooperation is carried out. Further development of the National Crisis Management System, conducting general and specific sector exercises with the participation of state, business and academic structures. Implementation of campaigns to form a basic level of cyber hygiene for vulnerable social groups. Building a system for research and education and certification of people and technologies in the field of cybersecurity.

Phase 2 (development - from capacity to capabilities): cyber-resilient institutions and a "cyber-secure" society.

Organizing the identified and created capacity in Phase 1 to implement **resilience at the level of individual organizations** and capabilities for coordinated response to cyber incidents and crises, systematic prevention activities. Institutionalizing a sustainable mechanism for interaction in large-scale cyber incidents and campaigns, threats from cyber and hybrid crises. Monitoring the overall cyber picture, building basic capabilities for operational and strategic analysis and assessment, operational and technical interaction with NATO, EU and other international networks.

Phase 3 (maturity): cyber-resilient society.

Effective interaction at operational and strategic levels in a national and international perspective (EU and NATO). Based on the model of engagement of all stakeholders and common interests, the Republic of Bulgaria prioritizes developing capabilities in both the state and private and research sectors in identified niches to achieve **leading positions** in the region and **specialization** in partner networks in the field of cyber resilience. The main activities in the three phases, the expected results and performance
indicators are defined in the Roadmap to the Strategy.

2.2. Principles

The fundamental values of the European Union apply equally in the digital and physical worlds. The same laws and rules that apply in other areas of our lives apply in cyberspace.22

The principles on which the Republic of Bulgaria's cybersecurity policy is developed and implemented are in line with the principles that guide EU policy in this area:

- **Protection of fundamental rights, freedom of expression, personal data and privacy -** Cybersecurity can be reliable and effective only if it is based on the fundamental rights and freedoms regulated by the Constitution of the Republic of Bulgaria and enshrined in the Charter of Fundamental Rights of the European Union, in particular: the right to respect for private life and the confidentiality of communications; the protection of personal data; the freedom to conduct a business; the right to property; the right to effective legal remedies and the right to be heard. On the other hand, the rights of the individual cannot be ensured without guaranteeing the security of networks and information systems;

- **Ensuring free and equal access to the Internet -** Limited or no access to the Internet and digital illiteracy put citizens at a disadvantage, given the high degree of penetration of digital technologies into all activities of society;

- **Democratic and efficient multi-stakeholder governance in the current Internet governance model as a factor for cybersecurity -** The digital world is not controlled by a single organization. A number of stakeholders, many of which are commercial and non-governmental organizations, are involved in the operational management of Internet resources, protocols and standards, as well as in the future development of the Internet. The existing governance model should be preserved and developed;

- **Shared responsibility for ensuring cybersecurity -** An integrated and coherent approach to allocating roles and responsibilities related to cybersecurity across all levels and bodies of government, citizens, businesses and institutions. All actors, whether public authorities, private sector representatives or individual citizens, must be aware of this shared responsibility, take action to protect themselves and, if necessary, provide a coordinated response to strengthen cybersecurity.

The update of the National Cybersecurity Strategy is being developed taking into account the following **additional principles:**

- legality and proportionality, proportionality and prohibition of excessiveness, as elements of the content of the rule of law - measures to increase cyber protection and costs should be commensurate with the relevant risks and threats;

- inseparability of cybersecurity from national security;
- consistency with the commitments and principles of cooperation and interaction resulting from the membership of the Republic of Bulgaria in the EU and NATO,

22 JOIN(2013) 1 final/07.2.2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

active participation in the creation of common capacity and capabilities for cyberspace protection;

• application of a comprehensive approach in building the cybersecurity system; • coordination in the activities of state institutions and organizations in
accordance with their competence;
• dialogue and broad cooperation between state institutions, business, represented by operators of essential services and digital service providers, research and academic organizations, industry, national, sectoral and cluster business associations, employers' and non-governmental organizations;

• openness, transparency and responsibility in the formation and implementation of
cybersecurity policy;
• effectiveness and efficiency of management and executive activities –
periodic assessment of the implementation of the Strategy, the level of cybersecurity and the relevant capacities and capabilities. Timely update of the Strategy and its Roadmap to address identified new threats and risks; • democratic and civil control over the cybersecurity system.

2.3. Priorities

The cybersecurity policy includes various EU and NATO policy instruments followed by the Republic of Bulgaria. Addressing cybersecurity challenges requires actions that stem from the following strategic priorities:

• achieving a sustainable cyberspace;
• reducing cybercrime;
• increasing the resilience of communication and information systems supporting defense and national security interests;
• stimulating research and innovation to develop industrial and
technological resources needed for cybersecurity;
• development of international cooperation and interaction.

2.4. Approach - a common effort, oriented towards results

Achieving cyber resilience at the national level requires coordinated actions on the security and reliability of all components and assets of cyberspace: **information, technologies, people, organizations and facilities,** design and implementation of communication channels, services and systems for their management, their connectivity and interoperability, as well as overall leadership and management.

The achievement of the objectives and activities within the individual phases is based on the identification, inclusion and active engagement of **all stakeholders.** It is essential to clearly define the roles of stakeholders with respect to assets and communication and information systems –

owner, manager, operator, user/client, supplier, etc., and for each role and the relevant business processes, the degree of digital dependence needs to be assessed, including in the future. **The main factors** for the successful and accelerated achievement of the goals of the Updated
Strategy are:

- Linkage of the Strategy's objectives with the priorities and goals of the national strategic and program documents, defining the vision and general goals of the country's development policies in the medium and long term;

- Effective and efficient leadership and management of the cybersecurity system in the country in implementation of the Strategy, ensuring the necessary resources and, first of all, human capital in the field;

- Consistency with horizontal and sectoral strategies and implementation of a comprehensive, complex approach to achieving security of cyberspace and the digital environment as a prerequisite for successful digital transformation of Bulgarian society, for modernization and widespread introduction of intelligent IT solutions in all spheres of the economy and social life;

- Identifying and engaging **all key stakeholders23** – clearly defining roles, responsibilities and achieving common agreement on priorities and activities across the three phases, consistently applying this principle across all regulatory and legislative frameworks, as well as public-private partnership models involving academia and non-governmental organizations;

- Introduction of effective **project and program management** for the implementation of the identified measures and assessment of the achieved results and capabilities –
Formulation of the activities under the measures as separate projects, oriented towards specific and measurable results, their synchronization in a portfolio for full building of functional capabilities, and harmonization and coherence with the Roadmap, regardless of the sources of funding;

- **Effective use of the experience and good practices** of leading partners in the EU and NATO, active inclusion in partnership programs and initiatives, and activation of partnerships in the region to build common capacity and capabilities, linking national and international projects and programs, integration into international cybersecurity networks and coordinated actions in cyber crises.

3. Areas and priority directions for action

Achieving **the strategic goal - a cyber-resilient society and state -** requires systematic and consistent policy and actions in the following key areas: establishing and developing a national cybersecurity system; achieving cyberspace resilience through network and information security; protection and resilience of strategic objects and primary administrators; effective counteraction to crime; cyber defense and protection of national security.

23 Multi stakeholder approach

3.1. Establishment and development of the national cybersecurity system, as part of the national security protection system

Goals

Objective 1: *Building a mechanism for strategic and operational planning and leadership, coordinated actions at* ***the political and strategic level*** *to develop the necessary capacity and capabilities for cybersecurity.* ***Objective 2:*** *Ensuring an up-to-date* ***cyber picture*** *and understanding of the situation in cyberspace and making timely and adequate decisions.* ***Objective 3:*** *Interaction for* ***effective and coordinated prevention, response and recovery.***

Cyberspace security is an inseparable part of national security. The Updated National Security Strategy of the Republic of Bulgaria24 indicates the vital and other important national interests, the necessary conditions and prerequisites for their realization. For the development and guarantee of a secure cyberspace, as one of the important national interests, **the National Cybersecurity System is being built,** which is an integral element of **the system for managing and protecting national security.**

The cybersecurity system ensures democratic and efficient governance of state and administrative bodies, public institutions providing public services, and sharing of efforts by persons performing public functions, managers of strategic objects of importance for national security, operators providing essential and/or digital services, citizens and their organizations. All participants have a shared responsibility to take action to protect themselves and, if necessary, to ensure a coordinated response in order to strengthen the overall level of cybersecurity. A growing number of organizations, including non-governmental and private sector organizations, declare a vital need and willingness to actively participate in increasing overall cybersecurity for the development of a single digital market and society. Capacity is being developed by software and ICT companies, research units, professional organizations, as well as individual specialists. This creates a national cybersecurity competence community, part of the EU community, which, with regulation, develops around the European Cybersecurity Competence Center and the national coordination centers.

The updated National Cybersecurity Strategy is a platform for unifying and developing activities and resources in **a common structure and processes for coordinated actions at all levels** - political/strategic, operational, tactical and technical, by covering and engaging all key stakeholders. The envisaged measures aim to **build and institutionalize a unified system** of responsibilities, processes and procedures for monitoring the general state of cyberspace, interaction and effective use of technical capacity for prevention, coordinated response and recovery, trend analysis and creation of capabilities for active and efficient countermeasures.

Priority directions for action

24 Updated National Security Strategy of the Republic of Bulgaria, State Gazette, issue 26 of 23.03.2018.

3.1.1. Policies, strategies and plans - strategic level

The main regulatory framework for the establishment and functioning of the National Cybersecurity System is **the Law on the Management and Functioning of the National Security Protection System (ZUFSZNS), the Cybersecurity Law (ZKS),** the legal acts of the EU, mandatory or legally binding for the Member States25 , as well as the international commitments of the Republic of Bulgaria, undertaken with international treaties that have entered into force, to which the Republic of Bulgaria is a party in NATO, the UN and other organizations. Certain aspects are also regulated in other laws - the Electronic Communications Law, the Electronic Government Law, the Electronic Identification Law, the Law on the State Agency for National Security (SANS), the Law on the Protection of Classified Information, the Law on Electronic Documents and Electronic Certification Services, etc., as well as in by-laws adopted for their implementation.

performance.

The formation of a unified cybersecurity policy is the responsibility of the National Assembly, the Council of Ministers and the President of the Republic. Functions and responsibilities for cybersecurity are distributed among the highest state bodies.
as follows:

The National Assembly of the Republic of Bulgaria ensures the adoption of laws and
other acts related to cybersecurity and exercises parliamentary control.

The President, in his capacity as Supreme Commander-in-Chief of the Armed Forces of the Republic of Bulgaria, receives comprehensive information on the status and development of the National Cybersecurity System, and upon the introduction of a "state of emergency", "martial law" or "state of war", he directs the activities to ensure cyber resilience of the state and military administration. The management of the National Cybersecurity System is carried out by **the Council of Ministers** in accordance with the Constitution, laws and subordinate

regulations and in compliance with the goals and priorities specified in adopted strategic documents. The Council of Ministers adopts and periodically updates the National Cybersecurity Strategy. In the Management Program of the Government of the Republic of Bulgaria for the period 2017-2021

[26]. The relevant objectives, guidelines and expected results of the establishment and development of the National Cybersecurity System are reflected in the sectoral programs and plans of the competent administrative bodies and their administrations. For the implementation of the Strategy, the Council of Ministers adopts a Roadmap and an Implementation Plan27 and monitors the achievement of the priorities and objectives, as well as the provision of the necessary resources for the implementation of the set activities. The Council of Ministers in its long-term program documents28

sets a deadline for building a fully completed integrated national cybersecurity ecosystem.

25 According to the Treaty on the Functioning of the European Union - Art. 288 et seq.

26 Adopted by Decision No. 447 of the Council of Ministers of 09.08.2017

27 Measure 162 of the Management Program of the Government of the Republic of Bulgaria for the period 2017-2021.

28 Vision, goals and priorities of the national development program Bulgaria 2030 and designation of leading agencies for detailing the strategy on individual priorities, approved by Decision No. 33 of the Council of Ministers of January 20, 2020.

The Security Council29 of the Council of Ministers analyzes the state of the national security protection system, prepares assessments and proposes solutions and actions regarding ensuring and protecting network and information security from attacks, including with regard to threat countermeasures and crisis/cyber crisis management capabilities, as an essential element of national security protection activities.

Coordinating actions at **the political and strategic level** for ensuring the achievement of the necessary capacity and capabilities for cybersecurity, is carried out by a permanent advisory body, **the Cybersecurity Council** under the Council of Ministers. The Council ensures cooperation between the competent state authorities, business, the academic sector, and non-governmental organizations in defining and implementing state policy in the field of cybersecurity. The composition and functions of the Council are determined by law30. The Chairman of the Council is a Deputy Prime Minister, appointed by the Prime Minister. The organization of the Council's activities is regulated by an act of the Council of Ministers31 .

The functions of **the Secretary of the Council** are performed by **the National Cybersecurity Coordinator32,** appointed by the Prime Minister. The National Coordinator, Under the leadership of the Chairman of the Cybersecurity Council, it organizes and manages the preparation/updating of **the National Cybersecurity Strategy** and **the Roadmap** to it, which are the basis for implementing the policy at a strategic level. Working groups may be established within the Council to prepare draft strategic documents and regulatory acts or other expert proposals on specific issues related to their competence.

The responsibility for developing adequate sectoral policies and/or strategies for achieving cybersecurity, planning and implementing measures for the development of relevant capabilities lies with the administrative bodies belonging to the executive branch, as well as any other body with administrative powers authorized by law, including persons performing public functions and organizations providing public services, as well as public and private entities and operators of critical infrastructures, providers of information and public electronic communications networks and/or services. All of the aforementioned actors have direct responsibility in their sector and shared responsibility and commitment for the effective participation in national measures and plans, the provision of relevant resources for the development of capacity and capabilities for the consistent achievement of network and information security, cybersecurity of the entire society, business and the state.

Criteria for a functioning cybersecurity system at a strategic level:

ÿ Completeness and consistency of adopted and entered into force legal and regulatory acts regulating the issues of institutional development of the relevant bodies and the interaction between them;

29 Law on the Protection of Cybersecurity, published in the State Gazette, issue 61/2015, in force from 01.11.2015, amended by the Amendment to the Cybersecurity Act, issue 94 of 2018 G.

30 Cybersecurity Act, published in the State Gazette, issue 94/2018.

31 Regulations on the organization and activities of the Cybersecurity Council, adopted by Council of Ministers No. 375 of 27.12.2019, published in the State Gazette No. 102/2019, effective from 31.12.2019.

32 See 6

ÿ Maturity of the bodies and structures, provided with sufficient resources to effectively and efficient implementation of their assigned activities and tasks;

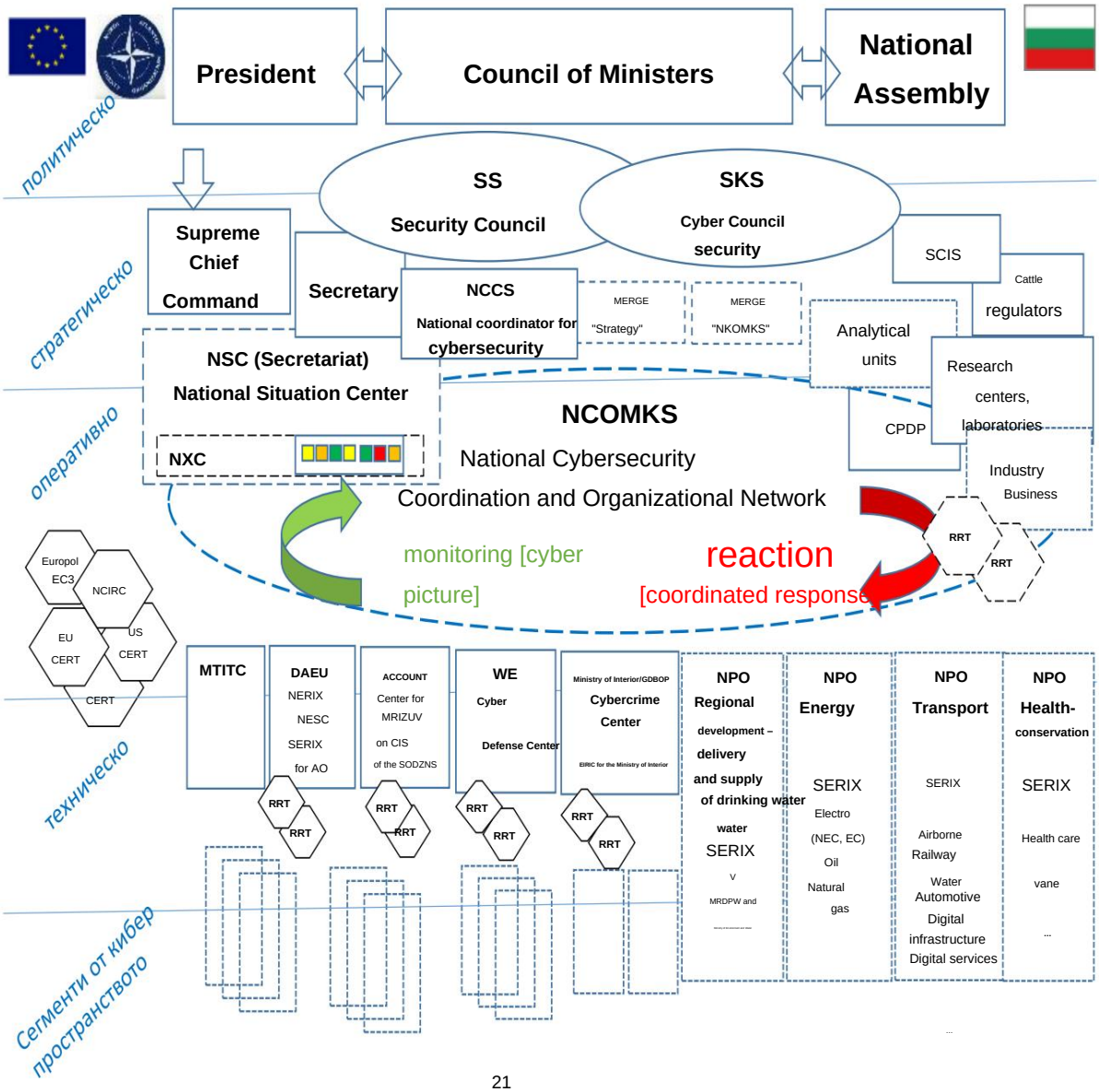
ÿ Priorities for the development of human, technological, infrastructural and organizational components have been derived; ÿ A Roadmap to the

Updated Cybersecurity Strategy has been developed, supported by a portfolio of projects and programs with effective management;

ÿ National Cyber Crisis Management Plan developed;

The approach to gradually achieving **a basic level of national cybersecurity** and a functioning operational system is based on optimal use of existing resources by building a national coordination and interaction network (in Phase 1). The flexible and open architecture of the model ensures the gradual development and addition of capabilities and structures to achieve **national cyber resilience** (Phases 2 and 3). The general model of the National Cybersecurity System is presented in Fig. 2.

Figure 2. Model of the national cybersecurity system



3.1.2. Operational Coordination Under the

Law on the National Security Council, **the Secretariat** of the Security Council is **the National Situation Center** of the National Crisis Management System. The National Situation Center assists the Council of Ministers in leading and coordinating actions for prevention, response, management and control of crises; interaction and coordination with the bodies of the European Union, NATO and other countries, as well as providing **a secure system for information exchange and continuous exchange of information for risk analysis and assessment.** To achieve Objective 2 and Objective 3 and for coordination at **the operational level,** an organizational network is being created - **the National Cyber Security Coordination and Organizational Network** (NCOCSN) with a relevant

technical platform, as well as **a National Cyber Situation Center** (NCSC) within the National Situation Center with the following main functions:

- Monitoring of the national **cyber picture** - state of cyberspace in the country, summarized information and indication of the status and smooth functioning of communication and information systems (including electronic communication systems, transmission networks, national and international information connectivity). For this purpose, a standardized protocol and multi-level status code are defined (in line with the established crisis codes, as well as those of the EU, NATO and partner networks), a link to shared technical information (of CSIRT/CERT33 also CSIRT/CIRC, etc.), analysis of possible causes and sources, impact assessment, as well as effectiveness of the measures and actions taken. Ability to assess in real time and make decisions on cybersecurity.

- **Coordinated reaction (response)** and operational interaction in large-scale incidents, complex attacks and crises – is carried out with organizational and technical means and is based on the current cyber picture, analysis of the situation and through technical protocol and organizational measures, information is provided on the situation at the national level, on possible combined threats and hybrid impacts, on potential kinetic and cascading ("domino") effects and recommendations are given for preventive actions at the operational and tactical/technical level, for activation of plans and actions from cyber defense, attraction of experts (from the working groups of the SCS, international, etc.)

The NCCS represents **the "nervous system"** of the National Cybersecurity System, and is being built and developed according to the model of **public-private partnerships** (PPP) with the involvement of all stakeholders from the public and private sectors. The NCCS is based on state organizations and bodies directly involved in the National Cybersecurity System (and in general in the protection of national security). The NCCS is open for the gradual inclusion of all interested organizations and institutions (state, business, academic and non-governmental) that manage, manage, operate and are responsible for various assets, components and segments of cyberspace. For this purpose, operational requirements are defined and implemented

33 **CERT** - Computer Emergency Response Team/Computer Emergency Readiness Team; CSIRT - Computer Security Incident Response Team; CIRC – Computer Incident Response Capability/Center (NATO).

compatibility, roles, responsibilities and operational capabilities based on a common mechanism, standardized processes and protocols for monitoring, prevention, response and
recovery.

Each interested organization provides capacity and capabilities for continuous monitoring of the status of the objects and segments of cyberspace entrusted to it with regard to aspects of cybersecurity and the functioning of communication and information systems (CIS) **(internal monitoring),** and teams for **immediate response** to cyber incidents or a violation of the functioning of CIS. These functions, organizationally and technically, are performed by centers and teams for responding to computer security incidents (CERT, etc.), in which permanent or ad-hoc teams and rapid response groups (RRT -

Rapid Reaction Team).

The organizations included in the NCMC interact interactively, continuously sending information about their cyber situation to the NCMC for the purposes of national monitoring and accordingly **receiving the current cyber picture for the country, an operational assessment** of the general situation, instructions and recommendations for coordination and interaction with other organizations. The functions of the NCMC are of **a coordinating network,** not of a centralized command center. It is the duty of each participant in the NCMC to **act immediately and autonomously** within the framework of their competencies, plans and capabilities. Based on the received general assessment of the situation and the overall cyber picture, these actions are adapted, expanded and coordinated with other centers and organizations. All participants take **preventive actions** and dynamically increase their state of readiness based on their own analysis and assessment, taking into account the national cyber picture and the recommendations under the NCMC. Monitoring the dynamics and development of the cyber picture in the NCMC network will be carried out by **operational analysis teams** (located in the CSIRT/CERT, or specialized units), which provide an operational assessment of trends in the development of cyber threats and negative consequences, recommendations for prevention and full recovery.

The NCOMKS model allows for the gradual inclusion of organizations with incomplete capacity, as some activities can be **delegated with technical and organizational measures** to other participants in the network. The NCOMKS is developing capabilities for ad-hoc formation of: a) **specialized combined**

teams for response to large-scale incidents of an interdisciplinary nature and/or hybrid attacks, with the involvement of research laboratories; b) specialized teams for investigation and detection of cybercrimes, teams for cyber defense, active counteraction to cyberterrorism and terrorist threats.

The architecture and operating model of the NCOMKS is based on the principle of a virtual network of interaction and follows the principles of the proven and flexible **"service-oriented"** model.[34]

The backbone of the NCCMCS is built on the basis of
structures, centers and organizations responsible for cybersecurity in various segments of cyberspace: • National RISKS within the framework of the State
Security Agency;
• National single point of contact within the SAEU;

34 Service Oriented Model/Architecture, Collaboration Networks

• Sectoral RISKS in the SAEU and at the National Competent Authorities, designated by decision of the Council of Ministers; • Cyber Defense Center (Mil CIRC – Computer Incident Response Capability) in the Ministry of Defense • Cybercrime Center in the Directorate General of Internal Affairs and the Ministry of Internal Affairs; • EIRIS in the Directorate General of Internal Affairs and the Ministry of Internal Affairs and the Ministry of Internal Affairs;
• Cybersecurity Center – CIS Directorate-Ministry of Interior;
• Center for monitoring and response to incidents with a significant damaging impact on the CIS of strategic objects and activities important for national security in SANS; • RISKS for classified networks in SANS; • National Counterterrorism Center in SANS;
• Analytical units; • Regulatory and accrediting structures;
• Research and other specialized units.

For the initial establishment of the NCCMCS, existing resources and centers are mainly used, expanded with the relevant organizational and technical means. Additional capacity and capabilities are gradually developed in the sectoral and departmental CSIRTs, as well as expanding the PPP base and mobilizing national and international resources. The NCCMCS includes, as a priority, **critical infrastructure monitoring systems, early warning and cybercrime centers, sectoral and business** CSIRTs.

The National Situation Center (NSC) houses a national center for continuous monitoring of the cyber picture in the country and ensuring a coordinated response - **the National Cyber Situation Center** (NCSC). The NCSC has functions for collecting, analyzing and immediately reporting received information in connection with the prevention, containment and management of crises35, as well as for coordinating actions and a comprehensive response to threats to national security as a result of a cyber attack. It provides an operational assessment of the generalized level of threat at the national level, disseminates recommendations for preventive actions and organizes coordinated actions in the event of a cyber crisis or an imminent threat of one. Operational and technical actions are undertaken by the relevant RISKS and rapid response teams (RRT). **The NCSC model** is in line with the recommendations of ENISA, ITU and NATO for a distributed mechanism of responsibilities and interaction on a federative principle, with a focus on the coordination of actions. It should ensure "openness" and easy integration of new participants, including at the regional and international levels. Business, academic and non-governmental organizations are actively engaged in the development of the NCCMCS by establishing and developing an effective PPP model.

The principles for the design and development of the NCMS and the requirements for organizations and monitoring centers are determined by the Cybersecurity Council in accordance with the development of the model and architecture of the National Cybersecurity System and the interoperability requirements.

The requirements for information exchange, technical and cyber protection of the NCCMCS are implemented according to developed rules, protocols and levels of confidentiality, which

35 Crisis - within the meaning of §1, item 3 of the Draft Law of the Law on the Management and Functioning of the National Security Protection System

also take into account the requirements for classified information with the assistance of state regulatory authorities36. The relevant requirements and access levels are regulated and applied to organizations and individuals by all participants and in compliance with the **"need to know" principle37.** This principle is developed in accordance with the new principles of sharing - **"need to share"38** and **"responsibility to share"39** to achieve an open nature of the NCCMCS network and effective inclusion of all participants (public and private organizations) to achieve cyber resilience at the national level.

3.1.3. National Cybersecurity Coordinator

The functions of the National Cybersecurity Coordinator (NCSC) are defined by law40. He ensures the connection between the two levels of the Cybersecurity System - the strategic leadership and the coordination system at the operational level, as well as the connection with the National Crisis Management System. The National Coordinator participates in the establishment and development of the NCSC and ensuring its reliability, security and sustainability, and in the establishment and development of the NCSC, as a separate structure within the National Situation Center41. To staff the

The National Cyber Situation Center with the necessary human resources is seconded by competent employees from ministries and departments under the Civil Servant Act or under special laws.

3.1.4. National Cyber Crisis Management System

Crisis management is an essential element of the activities for the protection of national security. A state of crisis is declared, respectively canceled, by a decision of the Council of Ministers. Crisis management is carried out by the Council of Ministers through the National Crisis Management System, which includes national, departmental and regional situation centers. These are structures that collect, analyze and immediately report received information in connection with the prevention and/or containment of crises, as well as for **coordinating measures and actions** for response, control and overcoming the crisis.

The National Cyber Crisis Management System is part of the National Crisis Management System42 and includes: engagement of the NCCMCS network, with the participating organizations, centers and response teams; the National Cyber Security Coordinator and the expert capacity of the NCSC in the Secretariat of the Council for

36 SCIS (State Commission for Classified Information), SANS (State Agency for National Security), and other specialized bodies

37 Need-to-know – a justified need to access specific information, regardless of the general access permission

38 Need-to-share – the source of information determines the need and recipients of information sharing (for example: to get help, you need to share the necessary information)

39 Responsibility to share (provide)

40 Cybersecurity Act, State Gazette No. 94/2018, in force from 17.11.2018.

41 The functions of the National Security Council are defined in Chapter Three of the Law on the Management and Functioning of the National Security Protection System, State Gazette No. 61/2015, in force from 01.11.2015.

42 Law on the Management and Functioning of the National Security Protection System (LMSPSNS), 2015

security at the Ministry of Defense. They ensure the activities of **the National Situation Center** for Crisis and Disaster Management, at the national level, in two aspects: **1) For preventing and dealing with**

cyber crises - continuous monitoring of the national cyber picture for early identification and assessment of the level of threats. In a state of increased threat of a cyber attack or one of a hybrid nature, formation of teams for analysis, response and recovery, with the involvement of experts from various departments and organizations, recommendation of preventive actions, escalation of warnings and coordination for the management of cyber crises; **2)** In case of **general crises** or **large-scale threats of a hybrid nature** (including disasters and accidents) - increased monitoring of the cyber picture in connection with the smooth functioning of the systems necessary for dealing

with crises, and prevention of their expansion into cyberspace (in interaction with the Unified Rescue System43 and other specialized crisis management systems with the appropriate level of protection and resilience). **Cyber crises44** in their life cycle follow the stages of any crisis: noticing, understanding and assessing, making decisions, terminating, recovering, learning lessons. There is also an analogy in the basic states - normal, incident, crisis. Due to their virtual nature and the diversity of events in cyberspace, they have a number of features, such as: a completely new type, unknown and constantly evolving in form and

nature of crises; measures, plans and processes for interaction and response differ significantly from those in "standard" crises; indications of an approaching crisis are difficult to observe directly (a combination of "unknown knowns" and "unknown unknowns"), and the transition from escalating incidents to a complex crisis may be within hours and minutes; they have no "territory" and limited space, they are difficult to identify and determine the source and scope; they can have a "kinetic effect" and be a major component of the implementation of a hybrid attack.

Cyber crisis threats most often manifest indirectly through signals of violations to varying degrees of the functions of the relevant communication and information systems and hence of the relevant services, activities and businesses. The procedures at the highest level **(declaration of a cyber crisis,** declaration of escalation, request and provision of assistance, international interaction) follow the procedures established in the National Crisis Management System and the relevant plans, but taking into account specifics such as speed of response, intensity and scale of the impacts, as well as the need for rapid and coordinated actions to limit the consequences. The procedures for action in cyber crises follow the guidelines of **the European Standard Operating Procedures (SOP)45** for interaction in cyber crises, the **Blueprint** concept for a European coordinated response to large-scale cyber incidents and

43 Disaster Protection Act, Chapter Three. Unified Rescue System in force from 14.10.2011, amended by SG No. 8 of 25 January 2011, amended by SG No. 39 of 20 May 2011, amended by SG No. 80 of 14 October 2011, amended by SG No. 68 of 2 August 2013, amended and supplemented by SG No. 53 of 27 June 2014, amended and supplemented by SG No. 14 of 20 February 2015, amended by SG No. 79 of 13 October 2015, amended and supplemented by SG No. 81 of 20 October 2015, amended and supplemented by SG. No. 51 of July 5, 2016, supplemented SG. No. 81 of October 14, 2016, supplemented SG. No. 97 of December 6, 2016, amended SG. No. 13 of February 7, 2017, amended and supplemented SG. No. 97 of December 5, 2017, amended and supplemented SG. No. 77 of September 18, 2018, amended and supplemented

SG. No. 60 of July 7, 2020. 44 Regarding the definition of “cyber crisis” see Appendix-Glossary

45 EU SOP's – European Standard Operational Procedure for cooperation during cyber crisis, part of the European Cyber Crisis Cooperation Framework (ECCCF). Commission Recommendation (EU) 2017/1584 and Council conclusions of 26 June 2018 on coordinated response to large-scale cyber incidents and crises

cyber crises of a cross-border nature46, the **NATO** model of interaction and crisis management. From these arise some of **the basic standard requirements** for the NCMCS network in order to ensure its interoperability and openness at the international level.

Cyber crisis management is carried out on the basis of **a National Action Plan47**

which is proposed by the Cybersecurity Council and adopted by the Council of Ministers. The plan develops activities for ensuring preparedness, prevention, detection, response, mitigation, recovery, international cooperation. Activities for coordination and interaction with the relevant **departmental and regional situation centers are planned,** as well as for engaging **the national competent authorities under the NIS and the relevant sectoral RISCS. The national, departmental and regional cyber crisis action plans** should be developed in sync with the relevant plans for **protecting national security and cyber defense.** The hybrid nature of cyber crisis threats requires **a comprehensive approach** to response and protection and the mandatory addition of an adequate **cyber focus in all crisis management plans,** as well as additional capabilities in the relevant organizations. **A coordinated response mechanism** will be established for timely preventive actions in the event of an imminent threat, as well as response to cyber crises . It is based on developed standard operating procedures and the capabilities of the RISCS and their specialized rapid response teams (RRT). To address national cyber and hybrid crises, a mechanism and capabilities are being developed for the formation and coordination of **national joint rapid response**

groups.

When the nature of the cyber crisis requires a shift to cyber defense,
activate the defense management system and defense plans.

3.1.5. Increasing the role and responsibilities of state structures and stakeholders Building an effective

National Cybersecurity System requires a review and redefinition of the roles and responsibilities of government agencies, the academic sector, business and non-governmental organizations, which includes:

- Improving interaction and coordination at the highest state level in determining **national policies and priorities** for cyberspace security – National Assembly, Government, President, Judiciary; • Regulating the responsibilities according to the roles of owner, manager, owner and operator for the relevant segments of cyberspace of **the ministries and departments** directly involved in the national security system or responsible for critical infrastructures, **the operators of critical infrastructures** and the resulting obligations for ensuring NIS, reliability and protection of CIS, creating an internal organization and technical

46 Blueprint Recommendation C (2017) 6100 final of 13.9.2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises.

47 National Cyber Contingency plan

capacity for monitoring their condition, recording incidents, responding and recovery;

- Review and allocation of responsibilities and functions for all segments of cyberspace at the national level and in relation to international commitments and cooperation, development of regulatory and incentive policies mechanisms;
- Preparation and **inclusion in the National Cybersecurity** and Shared Cyber Risk Management System for all organizations and stakeholders (state, business, academic/research, non-governmental organizations) – creating capacity and meeting the requirements for the national NCCMCS network, developing capabilities for coordinated response and interaction at the national, sectoral and regional levels.

3.2. Network and information security – the foundation of cybersecurity

Goals:

Network and Information Security (NIS) is the foundation of cybersecurity. It must be in full synergy and complementarity with the other two pillars of cybersecurity - law enforcement and cyber defense - in order to achieve a sustainable National Cybersecurity Ecosystem in the country. The main goal of NIS is to build a National Cybersecurity System, based on a set of tools and solutions to achieve a high level of network and information security. It must provide effective cyber defense and help strengthen the capabilities of networks and systems in the country to counter cyber attacks by criminals, cyber terrorists, hacktivists and even state-sponsored actors.

This should be achieved with appropriate measures at national, sectoral, organizational and individual levels in terms of scope, and at technical, operational and political levels in terms of their specificity. **The specific priority action lines** for the coming years, along which measures regarding network and information security should be developed and implemented, are the following:

3.2.1. Building an environment for cooperation and partnership

This environment should be built between public institutions, scientific, educational, non-governmental and business organizations, as well as individual experts who can contribute to raising the level of MIS in the country. This can be achieved by increasing the level of cooperation and partnership with all stakeholders (internet providers, companies and cybersecurity experts) for sharing information and expertise on the basis of the NCCMCS and through various other partnership events and initiatives.

3.2.2. Imposing a minimum common level of MIS at the organization level

This level should correspond to the existing risks to the security of the organization's information resources against the identified potential

threats to them. It should also include the imposition of the principle of **"cybersecurity by default"** when developing and allowing the exploitation of key information systems and infrastructures. Another essential aspect for achieving a minimum common level of NIS is the imposition of systemic control for taking appropriate cyber protection measures by organizations and the imposition of a unified systemic approach for assessing and mitigating risks in relation to NIS.

3.2.3 Strengthening the capacity of institutions with relevant roles and responsibilities with regard to NIS, according to the national cybersecurity management framework defined in the Cybersecurity Act

Strengthening the capacity of these institutions is of paramount importance, as they must assume leadership responsibilities in the field of NIS. The already established sectoral structures for NIS should be strengthened by imposing a sectoral approach with regard to operators of essential services (OES) and digital service providers (DSPs), while at the same time strengthening the technical and operational capacity and capabilities of the National RIS and the relevant sectoral RIS should be envisaged.

According to the Cybersecurity Act, the Council of Ministers delegates responsibilities in the field of cybersecurity to certain institutions. To achieve a cumulative effect, it is important to achieve a high level of integration of cybersecurity systems between these institutions, while strengthening their capacity. The schemes and processes of escalation and coordination between them at the strategic, operational and technical levels must be consolidated and played out in detail to achieve a high level of confidence in resolving incidents with a significant damaging impact, including cyber crises.

Taking into account the requirements for personal data protection, it is also necessary to increase interaction with personal data protection authorities and administrators in relation to threats of personal data compromise as a result of cyber incidents.

3.2.4. Integration of the National Cybersecurity System into European structures and initiatives in the field of NIS

The national cybersecurity system must include the establishment of the relevant structures and organizations in accordance with the commitments of the Republic of Bulgaria in the European cybersecurity structures, such as the National Single Contact Point under the NIS Directive, the National Cybersecurity Certification Authority, the National Cybersecurity Coordination Center under the provisions of the European Commission for the establishment of a network of cybersecurity competence centers and the European Cybersecurity Industry, Technology and Research Competence Center, etc.

3.2.5. Introduction of the European Cybersecurity Certification Framework

A relevant national organization must be established in accordance with the requirements of the EU Cybersecurity Act48 , which will enable European

48 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and cybersecurity certification of information and communication technologies

cybersecurity certificates and declarations of conformity of ICT products, services and processes to be recognized and used in all Member States, including Bulgaria.

3.2.6. Engaging the private sector in improving the level of NIS

The vast majority of network and information systems are privately owned or managed and operated by the private sector. Moving to the next stage of maturity requires joint work and commitment from the state and business to raise the overall level of MIS for the efficient implementation and expansion of secure and reliable Internet-based services. To achieve this goal, it is necessary to accelerate the transfer and adoption of good practices, technologies and proven models from the industry, as well as implement modern tools and platforms

for identifying and responding to incidents and security breaches, analysis, examination of evidence, tests and simulations, conducting pilot and test projects on the initiative and with industry resources. Private initiatives and projects to increase investment in MIS should be supported.

3.2.7. Ensuring a high level of cyber protection of critical information resources and infrastructure

It is necessary to increase interaction and cooperation between competent authorities regarding the cybersecurity of 5G networks, key SCADA systems, including transport infrastructures, etc. It is of particular importance to ensure a high level of cyber protection of key state information resources and infrastructures such as the State Emergency Management Agency, the European Energy Market Service, e-government information systems, etc.

3.2.8. Conducting information campaigns on cybersecurity and cyber hygiene

Raising the awareness of the population regarding cybersecurity and cyber hygiene will improve and raise the overall level of NIS. To achieve this, it is necessary to expand the scope of NIS cyber hygiene initiatives and campaigns to reach the maximum number of citizens and businesses in all spheres and with strong interaction between state, business and society. As a basic line regarding cyber hygiene, measures and incentives should be taken to integrate globally recognized good practices in the field of cybersecurity.

It is also important to strengthen the interaction between competent authorities and private business in the field of cyber hygiene by organizing joint campaigns of public and private providers of Internet-based services to introduce and publish their policies and measures to ensure MIS, cyber protection and continuity of services as essential elements of competitive advantages, transparency, balancing of regulatory mechanisms and market principles to achieve a safe and reliable space for end Internet users.

communication technologies. The national certification system including the National Cybersecurity Certification Authority, conformity assessment bodies, accreditation body, national scheme, etc.

3.2.9. Improving the skills and professional competencies of network and information security experts

The constant emergence of new and increasingly complex threats to

cybersecurity requires the continuous improvement of the competencies and qualifications of experts. This is achievable only with their regular participation in various courses on topics in the field of NIS. Another important part of maintaining skills and competencies, as well as improving teamwork and cooperation between all national structures in the field of cybersecurity, is regular participation in various exercises under the auspices of the European Union, NATO, the International Telecommunication Union and other international organizations, as well as in national ones. An indispensable part of improving qualifications is the organization of national exercises on various topics, which are consistent with current trends and threats in cyberspace.

3.3. Protection and resilience of strategic sites49 and primary administrators50

Main objective: Improving the protection and resilience of the communication and information systems of departments that are strategic objects, critical information infrastructures (CII) and primary data administrators and the primary registers maintained by them.

The high dependence of business, society and the state on CII, their cross-border interconnection and their interdependencies with other infrastructures, as well as the vulnerabilities and threats they face, increase the need to **consider their security and resilience from a systemic perspective,** as a front line of defense against failures and malicious attacks. The complex of risks targeting critical communication and information infrastructures has a diverse origin, being formed by human activity, natural disasters or technical failures. This heterogeneity often makes them highly specific, poorly understood and fully and/or insufficiently analyzed. The formed complexity of the risks and the poorly determined context in which they develop slows down and greatly complicates their addressing and management.

Another key problem arises from the increasing interdependence of information and communication systems with the systems of a number of critical infrastructure sectors, such as security, energy, transport, finance, healthcare, telecommunications, food and water supply, defence and many others51. Most of the information systems, services, networks and infrastructures form a vital part of the economy and public activities, either providing essential products and services or being the main platform for other **critical infrastructures** and allowing the exercise of the rights and freedoms of citizens. They are defined as **critical communication and information infrastructures,** since their disruption or destruction can lead to the collapse of the state and society and disruption of their normal functioning. In case of adverse impacts against

49 According to Council of Ministers Decree No. 181/2009 on the determination of strategic sites and activities of importance for national security

50 Within the meaning of Art. 2, para. 2 of the Electronic Governance Act

51 See COM(2009) 149, link COM(2005) 576 of the EC

these systems, the unforeseen negative consequences and possible cascading effects for other sectors and society can be many times greater in quantitative and qualitative terms than the benefits for which they were designed and created.

Priority directions for action::

- Development of a model for timely identification of critical national security information infrastructure;
- Integrate capabilities and procedures for active engagement in the management of the risk for CCII;
- Introduction of procedures for integrating society into information protection of the CCII through focused awareness raising;
- Expanding coordination and interaction with EU member states, NATO to minimize risks and threats against the CCII;
- Increasing the technical, administrative and organizational capabilities of the authorities involved in protecting the information systems of strategic sites and activities that are important for national security and of the primary data administrators and the primary registers maintained by them;
- Building capacity and capabilities for monitoring cyber incidents in the information infrastructure of strategic sites and activities that are important for national security;
- Development and implementation of specific **plans and procedures** for protecting the information systems of strategic sites and activities that are important for national security and of the departments, primary data administrators and the primary registers maintained by them;
- Based on partnership and mutual understanding of responsibilities, the heads of strategic objects and activities that are important for national security **update** the general and specific requirements and measures for cybersecurity, towards achieving cyber resilience, and covering the entire life cycle for managing cyber risks and implementing the entire complex of activities for identifying the organizational structure and assets, their protection, incident detection, response, recovery and relevant lessons and improvement52; • Update the standard operating procedures for risk management and neutralization of threats to CCII;

–

- Encourage and support the creation of sectoral or cluster organizations to share information and enhance collective cybersecurity in the area of critical infrastructures (ISAC/ISAO 53).

3.3.1. Improving the interaction between the state and operators of critical infrastructures – strategic sites and activities • Distribution of commitments and strengthening the cooperation of the state with the operators of CCII and CI, through interoperability agreements;

52 NIST: Framework for Improving Critical Infrastructure Cybersecurity (2014): Identify, Protect, Detect, Respond, Recover, also developed in standards and models such as ISO/ICE 2700x, COBIT, CCS CSC, CERT-RMM

53 ISAC/ISAO Information Sharing and Analysis Center/Organization

- Involve critical infrastructure operators in the processes of national crisis and disaster management arising from cybersecurity, in the construction of the overall security architecture. Develop their capacity and capabilities for crisis risk management by creating a functioning security system, including the designation of internal security authorities;

- Periodic review and timely updating of **cooperation agreements** between competent state authorities and operators of strategic facilities and activities that are relevant to national security and of primary data administrators and the primary registries maintained by them in the context of the development of challenges in cyberspace and, on this basis, amendment and supplementation of crisis action plans and cyber defense plans.

3.3.2. Development and modernization of critical infrastructure management and protection systems - strategic sites and activities

- Identifying new cybersecurity challenges relevant to
  to 5G communication connectivity, the Internet of Things;
- Priority **modernization of processes, technologies and systems** and improvement of protection and security of management systems such as
  ICS/SCADA54, adequate to modern cybersecurity requirements, in accordance with **internationally recognized standards** and models, relevant audit and certification;

- Identification, isolation of access and phased replacement of software, systems and components with expired manufacturer or supplier support (including operating systems, office suites, etc.), or obsolete, representing a particularly vulnerable and easy target for malicious actions, defects and dangerous instability.

3.3.3. Timely protection of new areas of cyberspace

The rapid and widespread penetration of digital technologies into everyday life and business also predetermines **the continuous expansion of the assessment of "criticality" of communication and information systems in line with the growing digital dependence,** which requires a mechanism for the dynamic expansion of the scope of requirements and measures for critical infrastructures and on developing socially significant electronic environments and platforms, such as various **e-commerce systems, online payment portals, social networks, payment machines, etc.**

search, cloud services and applications, online app stores55 , online media, etc.

Areas with high growth in the digitalization of business processes are **financial services, e-payments and digital currencies, the field of electronic commerce,**

54 Industrial Control Systems – ICS, Supervisory Control and Data Acquisition – SCADA ÿ ÿÿÿÿÿ
55 App-store ÿ ÿÿ.

healthcare and insurance, and others, which defines their communication and information infrastructures as critical. Regardless of whether these areas are formally included in the lists of CIs, their rapid development and entry into the lives of citizens and companies requires **timely integration into the National Cybersecurity System** and their coverage by the requirements and coordination mechanisms for cybersecurity. The implementation of the measures is based on a balance of the mechanism of regulation and self-regulation and **the addition of cybersecurity to the requirements and advantages in the competitive business environment.**

The aggravation of the situation with the fined and open Internet in conditions of geopolitical tension in recent years has been accompanied by targeted activities that harm international security and thwart the benefits of cyberspace for economic, social and political development. The decentralized architecture of the global Internet shows a high degree of resilience in terms of the ability to support a sharply increased volume of traffic in the conditions of the global COVID-19 pandemic. Bulgaria, as a member state of the EU and NATO, needs to be prepared for possible future destabilizing geopolitical or technical events that affect the basic functions of the Internet.

Ensuring the reliable functioning of the global network is a strategic objective, for which a common European policy is being developed and implemented, which focuses on taking convincing measures against cyber incidents and malicious online activities, as well as limiting dependence on infrastructure and services located outside the EU. This will require a combination of legislative measures and a review of existing rules to ensure a high common level of security of network and information systems in the EU; increasing investment in research and innovation; and seeking ways to deploy or strengthen essential internet infrastructures and resources, in particular the domain name system56. An important element in protecting key European and national digital assets is to be able to offer a secure communication channel for critical

infrastructure. The European Commission is already working with Member States to deploy a certified fully end-to-end secure quantum infrastructure, both ground-based and space-based, in conjunction with the secure government satellite communication system set out in the Space Programme Regulation57 . The EU government satellite communications, which are part of the Space Programme, will provide in the near future a reliable and cost-effective communication capacity to ensure missions and operations of critical importance to security and safety, which are managed by the EU and its Member States, including national security entities and EU institutions, bodies and agencies. Bulgaria has committed58 to work together with the Commission and other Member States on a secure and quantum communication infrastructure (QCI) for Europe.

56 The Domain Name System (DNS) is a hierarchical and decentralized system for naming computers, services, or other resources connected to the Internet or private networks. It translates domain names into IP addresses.
addresses needed to locate and identify computer services and devices

57 Proposal for a Regulation establishing the Space Programme of the Union and the European Union Agency for
the space programme COM(2018) 447

58 In February 2020, Bulgaria signed the EuroQCI Declaration for the development and deployment of QCI in the period 2021-2027.

3.4. Effective counteraction to cybercrime

Objectives: ***Objective 1:*** Establish an effective and efficient process for **prevention and protection, response, investigation and adequate law enforcement;**
Objective 2: **Improved operational capacity and capabilities** to counter cybercrime and cooperation at national, European and international levels.

Law enforcement and the fight against cybercrime is **the second fundamental pillar** of cybersecurity. The economic, material and moral damage resulting from cybercrime and malicious acts severely undermines trust in digital and electronic services and in the development of an open and democratic society and a dynamic and sustainable economy.

In parallel with the development of digitalization in the Republic of Bulgaria, the number and diversity of cybercrimes is increasing. Theft of personal and financial data carries a reputational risk for financial institutions, which contributes to the low level of reporting to the police. A significant part of cybercrimes today are related to cyberattacks and penetration of information systems, with the aim of blocking or stealing data to blackmail individuals and businesses. The nature of organized cybercrime implies a pronounced multinationality and cross-border nature in the activities of criminal groups. In many cases, cyber incidents, as events or a series of unwanted or unexpected events, are caused by criminal acts. **Broad** public awareness of the risks is of utmost importance for the prevention of crime in cyberspace. Addressing the problems related to the constantly developing forms of cybercrime is important for
all levels of education and general awareness, with attention to be paid to adolescents, who are increasingly "living" in virtual space.

Priority directions for action

3.4.1. Cybercrime prevention

- Increasing the level of public awareness about the status, structure and trends in the development of cybercrime and the causes and conditions that facilitate it;

- Timely informing citizens, businesses, and society about emerging cyber threats and the associated escalating opportunities for criminal attacks, so that all potentially affected are informed about the risks they face in the online environment and can take independent protective measures in advance;

- Strengthening cooperation with non-governmental organizations, business associations and communities, and educational institutions to develop and implement programs targeting different population groups in view of their role and vulnerabilities in cyberspace;

- Expanding support for networks of researchers who collect information on the uses, risks and consequences of online technologies on children's lives. Focusing prevention on the protection of adolescents in the online environment, in relation to their addiction to the Internet, their dependence on social networks, as well as their low awareness of the various forms of cybercrime and the sanctions provided for the committed punishable acts. Significantly limiting the dissemination of materials containing cases of child sexual abuse;

- Defining specific measures and actions for preventive protection against existing and emerging threats, and coherence with the implemented cyber hygiene measures, to achieve an overall high level of MIS, including with regard to unknown impacts and attacks;

- Implementation of adequate measures for individual prevention and protection in order to prevent harmful effects on potentially threatened subjects/objects;

- Increasing the legal culture of end users regarding the punishability of typical acts committed in cyberspace. Annual organization of **a cybercrime prevention week;**

- Conducting awareness campaigns to limit the use and distribution of unlicensed digital products (software, media), which constitutes a crime in terms of copyright, and is a serious threat to the distribution of malicious code and subsequent illegitimate actions (including “complicity” in large-scale cybercrime, through botnet networks, stolen identities, etc.). Strengthening prevention by widely publicizing the results of law enforcement operations, as well as eliminating the practice of using unlicensed software and the absence of minimal cyber protection measures in public institutions under the personal responsibility of their leaders;

- Widely promoting in the media the Cybercrime Center at the Directorate General of Criminal Investigation and Prevention-Ministry of Interior and its mission to detect, investigate and document computer crimes. Increasing the legal culture of citizens regarding their public obligation to report cybercrimes that they have become aware of or have suffered from.

3.4.2. Increasing the administrative, organizational and technical capacity and capabilities of the competent structures

The steady trend towards an increase in the number of computer and computer-related crimes, the increasingly easy access of offenders to the means to commit such crimes, including through the use/provision of cybercrime services59, limits the ability of law enforcement and law enforcement authorities to respond. The effective performance of their legally assigned functions of detection, investigation and prosecution

59 Now also provided as a service - Cybercrime-as-a-service.

of offenders, requires increasing their administrative, technical and organizational capacity and abilities **through the implementation of complex measures:**

- Institutional strengthening of existing specialized structures in the Ministry of Interior, directly involved in countering cybercrime through:
  - o refining their functional competence;
  - o providing the necessary human resources and modern technical means and technologies;

- Strengthening information exchange with the European Cybercrime Centre at Europol, with **partner structures and organizations** to achieve effective and timely investigation of cybercrimes of a cross-border nature; • Increasing the capacity and capabilities for effective participation in cross-border joint cybercrime investigation teams with services and bodies of other

countries and international organizations, formed under the leadership of the VCP;

- Active participation in various international and regional initiatives and projects to combat cybercrime;
- Effective use of training opportunities within the framework of bilateral law enforcement cooperation, in the training courses organized by the European Union Agency for Law Enforcement Training;

- Through a PPP agreement in the field of training, ensuring **high levels of competence** of police officers; implementing the transfer of experience and good practices regarding the use of new methods for threat analysis and risk assessment; implementing innovative tools in the collection and investigation of evidence of crimes in cyberspace.

3.5. Cyber defense and national security protection

Goals:

***Goal 1: Protection and counteraction** to various types **of attacks and organized actions of a destructive nature in cyberspace** that threaten the security and stable functioning and development of the state and society, as well as partner countries by virtue of mutual agreements and commitments.*

***Goal 2:** Achieving resilience to organized large-scale hybrid impacts at the institutional and national level, guaranteeing and maintaining the basic functions of the state (government, business, citizens) and restoring normal activity.*

The measures to achieve these goals and their phased implementation will lead to increased security and sustainable and competitive development of civil society, business and the state in cyberspace. They are organically linked to the development of the National Cybersecurity System, with the construction of the model for

coordination and interaction at the national level and ensure development in **two aspects:**

- Protection and cyber resilience of communication and information systems, networks and the management organization of **the national defense and the armed forces** of the Republic of Bulgaria, and implementation of commitments and

active participation in the development of collective defense capabilities in **shared cyberspace** with partners and allied countries from NATO and the EU;

- Ensuring **an effective mechanism for rapid and coordinated response** to large-scale cyber and hybrid attacks and crises with possible catastrophic consequences, as well as resilience of systems for managing vital resources for the functioning of the state and society in emergency situations. Cyber defense is **the third fundamental pillar** of cybersecurity according to

European Cybersecurity Strategy (2013).

Priority directions for action:

3.5.1. Cyber defense and armed forces

The use of cyberspace as a fifth operational domain for conducting operations and the responsibilities assigned to the Minister of Defense by the Cybersecurity Act for protection and active counteraction to cyberattacks and hybrid impacts on defense management systems and the armed forces require the implementation of interrelated and complementary measures to ensure and develop administrative, technical and organizational capacity and capabilities for cyber defense, compatible with those of NATO and EU allies, as well as common ones at the alliance level:

- Establishing and developing a sustainable organizational model for coordinated and effective leadership, planning and management of cyber defense at the strategic, operational and tactical levels;
- Integrating cyber defense as an element of strategic planning in defense capability building programs and in plans for conducting operations by the armed forces;
- Development of a cyber defense center (milCCIRC) to ensure continuous monitoring (24/7) and assessment of CIS security and formation of a complete operational picture of cyberspace;
- Development of cyber defense teams, including for timely response to cyber incidents and attacks and restoration of critical communication and information services for the implementation of the missions of the armed forces;
- Implementation of investment projects for cyber defense and use of the opportunities of the Republic of Bulgaria's membership in NATO and the EU, as well as of support programs and bilateral cooperation with other countries for participation in joint initiatives and development of common capacity and capabilities;
- Building expert capacity in cyber defense by developing and utilizing the capabilities of the national and military education systems and increasing the knowledge and training of personnel for conducting cyber operations, through participation in courses, training and exercises in a national and international format;
- Effective use of the membership of the Republic of Bulgaria in the NATO Cyber Defence Competence Centre (NATO CCD CoE), as well as the capabilities of the NATO Competence Centre for Crisis Management and Disaster Response in Sofia60 for the development and upgrading of specialists in

60 NATO CMDR COE – NATO Crisis Management and Disaster Response Center of Excellence

planning and conducting operations in cyberspace and studying modern persistent threats, attacks against CI, methods and protection systems;

- Coordinated sharing of good practices, information on cyber incidents and mutual assistance with state institutions, NATO and the EU, cooperation with business and the academic community;

- Development of research and applied science activities to create sustainable systems and models in the field of cybersecurity, as well as improving interaction with scientific and research organizations and active inclusion in international programs of NATO and the EU through research projects;

- Implementing a comprehensive and holistic approach to the formation and development of a body/s for assessing the conformity of cybersecurity products/means, processes and services of national importance, in accordance with Regulation EU 2019/881 of the European Parliament and of the Council;

- Adaptation and implementation of the EU and NATO model for pooling and sharing resources at the national level, specialists, technologies, base and development of forms of engagement – using the armed forces reserve mechanism to create a specialized "cyber reserve" and other forms of engagement of cyber specialists from industry, academia and professional circles.

3.5.2. Countering hybrid threats and cyberterrorism

- Implementation of measures and tools to **increase awareness** of the overall threat environment and the state of the cyber landscape at the national level (based on the national NCOMKS network), development and implementation of a unified and reliable system of indicators for operational assessment, recognition and warnings at the national level (as well as in the NATO and EU networks);

- Implementation of measures for increased protection, resilience of monitoring and control systems at national borders, checkpoints, for coordinated port management (in accordance with National

  Single Window)61 , airports, air traffic control, and ensuring continuous operational interaction with the relevant structures of the EU, the Schengen Area, NATO and other partner organizations and networks;

- Development of combined measures and tools for **identifying and associating the sources and perpetrators** of hybrid actions (which predominantly use ICT and cyberspace as a means of influence);

- Development of capabilities for preventive and active coordinated countermeasures to limit harmful consequences and prevent emergency situations;

- Establishing specific operational procedures and means for **rapid action in the event of particularly intense aggressive and destructive impacts** such as terrorist acts (of a cyber or hybrid nature) targeting CI and creating capabilities for forming rapid response teams (RRTs) with mixed cross-sector and international expertise;

61 Directive 2010/65/EU National Single Window (NSW) for maritime transport

- Establishing criteria and procedures for management, decision-making and **preparedness for response in emergency situations** and relevant organizational and technical means for: implementing **continuous awareness and control of the situation at the national level** across the entire range - a state of increased intensity and scale of the incident, the threat of a cyber and hybrid crisis, emergencies with characteristics and degree of possible impact on the scale of cyber or hybrid wars; coherence, coordination and testing of mechanisms for **receiving and providing international assistance and collective actions.**

3.5.3. Cyberrecognition

- Establishing mechanisms and technical means to maintain an up-to-date picture of possible threats of different scale, sources and nature (cyber, hybrid), development trends in a geopolitical context and relevant analysis of the national cyber picture, integration with the National Cyber Security Center;
- Development of capabilities to assist in identifying the sources of impacts during attacks ("attribution") and undertaking adequate forms of protection and countermeasures.

4. Interaction between state, business and society, improving information sharing

Goals:

Development ***of an effective mechanism and environment for information sharing and interaction between all groups of stakeholders*** *to achieve an open, secure and safe cyberspace*

The goal requires identifying interests and expectations in the short and long term, allocating responsibilities and commitments. Responsibility for the reliability and security of cyberspace is shared and requires sharing information, building joint capacity, increasing the common understanding and "culture" of cybersecurity and striving for cyber resilience, as well as the joint development of a secure, reliable and attractive cyber environment for the development of a competitive economy and society.

To achieve this goal, the Cybersecurity Council under the Council of Ministers establishes a **High-Level** Working Group on improving interaction and information sharing between state institutions, business, the academic community (BAS and the Council of Rectors), NGOs in the field of cybersecurity. The Working Group should prepare and monitor the implementation of the program "Improving interaction and information sharing between state, business and society", financed by the state and business and approved and reported annually by the Cybersecurity Council.

Priority directions for action:

4.1.Establishment of effective mechanisms for sharing information and engagement of all stakeholders

• Identifying and engaging all stakeholder groups to determine the need, opportunities and interests for sharing information on the occurrence and assessment of risks from the impact of incidents at different levels: **strategic, operational, technical;** identifying, analyzing, and coordinating the adoption of threat management measures; continuously reviewing and improving incident response measures and recovery;

• Determining **the target roles and interests of the various stakeholder groups** and establishing an adequate **form of participation in the National Cybersecurity System** - from assistance in identifying measures to implement the set goals, through participation in capacity and capability development projects, to full inclusion with assuming responsibilities, participation in PPPs;

• Stimulate and support the creation of adequate group and **collective platforms for information sharing and collective response** - based on a sectoral approach (for individual sectors and sub-sectors - e.g. energy, transport, finance); on a cluster principle - business and territorial connections and dependencies; on the basis of supply chains and more generally - for value creation. Development of appropriate packages and incentives for all stakeholders;

• Adaptation, development and implementation of forms and methods of institutionalization - **establishing sectoral and cluster centers and organizations** for information sharing and analysis (based on the experience of the US and EU countries62 and the various ISAC/ISAO models63) and expanding them from an information sharing mechanism to active inclusion in the national NCCMCS network and effective participation in collective protection and counteraction - supplementing them with relevant operational and specialized technical capabilities and response teams/centers;

• Development of methods and tools for building **trust for information exchange.** Use of protocols and rules, according to established international and national standards and models, to achieve voluntary, but highly engaged and responsible participation64 . • Development of **a national classification and common "language"** for sharing sensitive information, harmonized with international norms and practices, with national legislation and consistent with the development of all aspects of cyberspace – threats, incidents, response and preventive measures, risk assessment and levels of preparedness, equivalent levels of information sensitivity (in national and international aspects). Coordination of requirements for information channels, sources of information and responsibilities65, which would stimulate the inclusion of public and private

62 USA, Kingdom of the Netherlands, etc.

63 ISAC – Information Sharing and Analysis Centers, ISAO – Information Sharing and Analysis Organizations

64 Cybersecurity Strategy of the Kingdom of the Netherlands - "Voluntary, but not without engagement"

65 E.g. ISAC/ISAO traffic light-based (TLP) limited sharing levels; threat level codes "green-yellow-orange-red" (weather, disasters) – widely used in national and international networks

organizations in the national NCCMCS network and their commitment at the operational and technical level to deal with incidents and crises;

- Defining and implementing a common package of measures to ensure the security and **reliability of information channels,** in accordance with the measures to enhance MIS - levels of protection and encryption, segmentation and regulated access, enhanced security measures, such as HTTPS-only, domain authentication (DNSSEC) and other additional recommendations of international Internet organizations and partner networks and organizations;
- Establishing, institutionalizing and accelerating the development of **an effective public-private partnership for cybersecurity** as the main mechanism of interaction and commitment for the construction and expansion of the NCCMCS;

- Active interaction and inclusion in the European initiative for a contractual "Public-Private Partnership for Cybersecurity"66, development of the "Digital Single Market"67 and NATO networks and programs68 - engagement of ICT associations and clusters, research and academic organizations, as well as national, sectoral and cluster business associations, industrial and employer organizations, non-governmental organizations.

4.2. Focus on medium and small businesses

In 2019, the Digital Economy and Society Index (DESI) shows that only 6% of small and medium-sized enterprises in Bulgaria sell online, and according to the National Development Program – Vision, Goals and Priorities Bulgaria 203069, their share should reach 12% by the end of the period, compared to an average of 17% for the EU. In order to ensure conditions for accelerating the digital transformation of small and medium-sized businesses, it is planned that enterprises will receive support in the field of digital technologies and information security.

Priority directions for action in the field of cybersecurity:

- Initiating focused programs, adding the main measures to the programs for the development of **the competitiveness of small and medium-sized businesses, including micro-enterprises,** to raise awareness and "cyber culture", including specific packages of recommendations and requirements, so as to ensure **effective participation in the single digital market** (at national and international level), awareness of digital dependence on information channels, supply management, security of communication and information systems. Implementation of basic or adapted for small and medium-sized enterprises (SMEs) standards for information and cybersecurity at the enterprise level;

- Development of mechanisms for the promotion and organized **inclusion of small and medium-sized enterprises in networks for information sharing and prevention** based on a sectoral or cluster approach, conscious sharing of **cyber risks**

66 European cPPP – Contractual Public-Private-Partnership for Cybersecurity (2016) industrial research and innovation – ECSO: European Cyber Security Organisation

67 Digital Single Market (DSM) strategy of European Commission (EC) and Rolling Plan 2015 for ICT Standardisation

68 NATO NICP – NATO Industry Cyber Partnership http://www.nicp.nato.int/index.html

69 Approved by Decision No. 33 of the Council of Ministers of January 20, 2020.

across supply chains and the entire flow of interconnected digitalized businesses and markets;

- Defining and implementing an adapted approach to stimulate initiative, self-regulation and following the culture of **"digital leaders"** - development of the cyber component in business relations and communications and use of typical business ecosystems: "small for small" (small businesses and citizens are served by small software and IT companies, without specific focus and attention to cyber aspects), "small for big" (small companies participate predominantly in supply chains and contribute to overall cybersecurity, or "insecurity") - active engagement of business and ICT associations, priority support from state institutions, national and international programs;

- Organizing specific sectoral and cross-sectoral **simulations, exercises or drills** with the aim of increasing the knowledge and engagement of small and medium-sized businesses and creating conditions for their inclusion in the scope of national and international exercises or drills.

4.3. Establishing a common communication strategy for awareness on cyber impacts and countermeasures

- In interaction with all stakeholders, develop **a common strategy and recommendations for communication and public sharing of information** related to incidents and consequences, with competent authorities achieving the necessary balance between the public interest in being informed about the threats and possible commercial damage and the damage to the reputation of public administrations and market participants related to the incidents, as well as ensuring adequate sanitization of information and confidentiality until the breaches are remedied;

- All organizations and institutions with responsibilities for management, management, exploitation and development of various segments and resources in cyberspace should establish internal communication policies, procedures and mechanisms that provide timely management information to management on cybersecurity threats and the status of the systems and resources entrusted to them, situational assessment in the context of the national cyber picture (supported by the National Cyber Security Council), as well as timely coordination at the management level and through information sharing platforms in an appropriate format for timely information to citizens and the public through electronic media, social networks and other information channels.

4.4. For a safe, free and trustworthy internet environment

- The competent state institutions, in broad cooperation with non-governmental organizations70 and based on the recommendations of global Internet organizations, should continue to develop the management and administration of
  activities related to management and access of citizens and businesses to the Internet

70 Internet Society, ICT and software associations, Internet providers and electronic service providers, business and employer organizations

connectivity and information, by developing an effective regulatory and self-regulatory mechanism ensuring the balance between accessibility and reliability, security and confidentiality, protection of personal data and sensitive information and activities in the interest of national and collective security - particular attention should be paid to preserving informal, trusted and highly public channels for sharing information between market participants, as well as between the public and private sectors;

- Adaptation, anticipatory development and **implementation of the recommendations of international Internet institutions and organizations, so that** the democratic development and management of the Internet space in the country places the Republic of Bulgaria among the leading countries in the world with a fully developed infrastructure for **secure encrypted communication and validation of Internet domains** (such as the "https-only" and DNSSEC initiatives);

- Introduction of measures to ensure **reliability, accessibility and security of open data** – application of specific requirements and standards to providers (public and private) and open data-based systems and services71 .

5. Development and improvement of the legal and regulatory framework

The specifics and dynamics of the development of society and the transfer of key activities to cyberspace require **an adequate, modern and adaptive legal and regulatory framework** for defining the roles and responsibilities of participants in cyberspace, so as to ensure effective and efficient interaction between all stakeholders, protection of values and provision of a secure and reliable environment for sustainable development of citizens, business and the state. In the process of digital transformation, the economy and society are more vulnerable to cyber threats and cyber attacks. Cybercrimes cover a wide range of criminal activities that have a pronounced multinational and cross-border nature. In these conditions, law enforcement authorities must have reliable legal instruments for a coordinated and joint response to threats.

The development and improvement of the legal and regulatory framework is based on the principle of compliance and proportionality of the normatively introduced measures / requirements / standards to the identified threats and risks, as well as the capabilities, scale and scope of the different categories of organizations (public, business, civil).

Goals:

Objective 1: *Improving the regulatory framework in line with the dynamics of public relations in the field of cybersecurity. Timely transposition of EU legislative instruments into the domestic law of the Republic of Bulgaria.*

71 In implementation of Directive (EU) 2019/1024 on the free access to data

Objective 2: *Adapt the political and legal framework to new technological trends and emerging technologies.*

Priority areas of action

• Introduction of the acts of European Union law in the field of cybersecurity into the national legislation; • Development and improvement of the legal framework for regulating
cybersecurity requirements and control over their compliance in order to prevent and minimize the impact of attacks and incidents affecting NIS; • Improvement of the regulatory framework in the field of protection of information and communication systems **of critical importance for the operation of strategic objects** and activities of
importance for national security;

• Adoption of legal changes to **ensure effective investigation and prosecution** of cybercrime in view of their specificity, including as a manifestation of hybrid impacts, in order to ensure reliable protection of the rights and legitimate interests of citizens, businesses and the state, and to improve cooperation and joint response at EU level and in the wider international context;

• To ensure high-quality and accessible services of public interest in the field of cybersecurity, establishing a regulatory basis for **long-term contractual cooperation** with the participation of public and private partners in the construction of technology parks, centers of excellence, centers of competence and in the development of the NCCMCS and the relevant mechanisms for sharing information and responsibilities;

• Studying foreign experience in the development of the legal framework in the field of cybersecurity and undertaking anticipatory legislative initiatives in relation to the dynamics in the development of products, services and processes, as a result of new technological trends and emerging technologies;

• Implementing a comprehensive and holistic approach to developing **regulatory regimes/mechanisms,** as well as supplementing existing ones in the direction of cybersecurity. Implementing a balanced approach between regulatory and self-regulatory regimes through:

- o **legally regulated** minimum mandatory requirements for MIS;
- o **a combined approach** combining mandatory regulatory requirements and voluntary sector regulations and imposed practices; o **voluntary mechanisms** applicable to small and medium-sized businesses, introduced on the basis of awareness, cyberculture, informal rules and recommendations.

• Stimulating the development and implementation of **assessment (audit) and accreditation** schemes of organizations, capabilities and systems: o at the level of organizations (public and private) and specialists;

- o at the level of sectors and national security system;
- o at the international level – in accordance with the requirements and standards, certification and accreditation for interaction with the systems of the EU, NATO and other partner organizations and countries.

- Promote the widespread implementation of the European framework72 for **the certification of** ICT products, services and processes to address the potential negative impact of vulnerabilities. Their identification and remediation play an important role in reducing the overall cybersecurity risk, thereby providing important benefits for citizens and businesses.

6. Increasing competences and capacities and stimulating research and innovation in the field of cybersecurity; raising awareness

Goals:

Objective 1: *Achieving high* ***awareness among all*** *stakeholders and* ***a shared understanding and assessment of threats*** *in cyberspace in relation to the growing general dependence on digital technologies and the need for adequate measures at all levels to achieve information and cybersecurity, and the development of a common cyber culture.*

Goal 2: *Incorporating aspects of cybersecurity and acquiring adequate competencies in* ***all levels and forms of education and training*** *to create specialists and leaders for the secure and sustainable development of the digital economy, society and government.*

Objective 3: Capacity development and *an enabling environment for the development of research and innovative applications to transform the Republic of Bulgaria into* ***a leading center for the development of cyber-resilient systems of the future in cooperation with EU and NATO allies.***

Efforts in this area are subject to the application of an optimized digital transformation model, with the implementation of change programs in 4 quadrants, in two steps of the change spiral:

- Academic sector
  - o Cybersecurity research;
  - o Education and training.
- Administration
  - o Policy development;
  - o Acquisition of abilities.
- Digital systems/services operators
  - o Defining cybersecurity requirements;
  - o Operating the acquired capabilities - ensuring cybersecurity.
- Industry
  - o Development of new systems and services for cybersecurity;

72 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and information and communication technology cybersecurity certification. According to Article 58 of that Regulation, each Member State shall designate one or more national cybersecurity certification bodies.

o Production/provision of systems and services.

At the same time, the definition of digital transformation, as a simultaneous and harmonized change of processes, organizations, technologies and people in the new digital operating environment, requires the definition of the scope of research -
processes, organizations, technologies, as well as the focus of training people around processes, organizations, technologies with a unified focus on cyber resilience.

The measures are focused on the academic and non-governmental sectors in interaction with the administration, operators and industry.

Priority areas of action

6.1. Research, innovation and digital leadership

- Stimulating the development of research and applied science in the modern and challenging areas of information and ICT security73
  and the creation of sustainable systems and models in line with the areas of the Strategic Research Agenda for Cybersecurity (EU)74 – maintaining
  at a high level of international cooperation with leading world centers and specialists with a focus on hot and current areas in relation to current and future challenges, technologies, infrastructure development, methods and models of use - European programs, networks (coordination centers), including for related areas - quantum computing, supercomputers, artificial intelligence (AI), etc. as well as for new technologies with NATO; • Commitment of all stakeholders to identify promising and critical areas and implement productive connections and interaction between scientific and applied research centers, academic units, leading software
and ICT companies, and academic units in various sectors and linking **master's and doctoral programs with real business and industrial applications** to form a national (academic) cybersecurity community for participation in the Digital Europe and Horizon Europe Programs through the National Cybersecurity Coordination Center.

- Creating effective mechanisms for engaging scientific and research potential (both in Bulgaria and abroad) to find **innovative solutions for the activities of the state and the public sector** - e-government and services, e-identity security and e-voting, encryption, security of cloud and mobile services, and other cybersecurity issues, as well as creating conditions and programs for financing accelerated development and implementation;

- Priority development and use of support mechanisms (national, European, bilateral programs) and stimulation of international cooperation in connection with the priority development of the digital economy and

---

73 ICT security - ICT products, ICT services and ICT processes in the field of cybersecurity - see in Art. 2, item 12, item 13 and item 14 of REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

74 ENISA: Strategic Research Agenda - https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-final-v0.96/view and connection with cPPP (Contractual PPP on CYBER)

information society in Bulgaria. Development and stimulation of **PPP forms and clusters** for the creation of mixed research and application laboratories, technology parks and centers, which will create opportunities and support the creation of competitive and secure ICT solutions, products and services, as well as support the rapid and safe introduction of new digital technologies into business and society. Stimulation of digital entrepreneurship, creation of business incubators for **competitive start-ups in the field of cybersecurity.**

6.2. Capacity development and shared skills

- Development and expansion of the scope of programs for **technological development of the industry, modernization and smart specialization75** in the field of digital economy and services – stimulating the development of systems with cybersecurity design and solutions, guaranteeing adequate levels of cybersecurity and protection, building and developing the relevant **industrial, corporate and professional capacity** with the creation of **a national system for certification76** of the cybersecurity of ICT products, processes and services and for accrediting the systems and services in the administration and industry.

–

- Identifying an appropriate entity/structure/, nominating it and obtaining an accreditation decision from the European Commission to perform the functions of **a National Coordination Centre (NCC) for the purposes** of the relevant EU Regulation, after its entry into force77. The NCC must possess or have direct access to technological expertise in the field of cybersecurity and be able to effectively attract and coordinate with the industry, the public sector and the research community. In addition, it must have the capacity to support the European Expertise Centre and participate in the Network of National Coordination Centres established in implementation of the said Regulation with the mission: to preserve and develop the necessary technical and industrial potential related to cybersecurity to protect the digital single market; to increase competitiveness and turn cybersecurity into a competitive advantage for other sectors.

- Priority development of joint initiatives, programs and projects in new areas of the digital economy and digitally dependent society (security of cloud platforms and services, mobile and smart devices, internet-connected devices, and relevant applications) – use of PPP mechanisms, European and international programs for the construction of **technology parks, centers of excellence** and centers of competence (such as the laboratories and innovative ecosystem being built in Sofia Tech Park,

75 Innovation Strategy for Smart Specialization of the Republic of Bulgaria 2014-2020 and the process of smart specialization, adopted by Decision of the Council of Ministers No. 857 of 03.11.2015; updated version 15.10.2015

76 In implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification

77 Regulation of the European Parliament and of the Council on the European Cybersecurity Industrial, Technology and Research Competence Centre – see https://www.consilium.europa.eu/bg/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/ and https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:ST_12104_2018_INIT

applied centers and laboratories at the Bulgarian Academy of Sciences, universities, centers and laboratories in companies and business organizations, startup companies) – **coordination and concentration** of the created capacity, base and competencies to effectively support and increase the competitiveness of the industry through testing for cybersecurity breaches, simulation environments for checking and increasing resilience to attacks and breaches and solving tasks and challenges defined by business and the state on the basis of a single

system:

- o for early warning of cyber incidents;
- o from connected cyber polygons;
- o for assessing and managing cyber risk within sectors and across sectors.

• Creating an effective **mechanism for sharing resources, capacity and skills** between the private, public and academic sectors based on mutual interest and a common vision and development strategy - taking into account the technologically leading role of business and the need to create an appropriate environment for development and support from the state and smart growth and development programs;

• Engaging large software, ICT companies and multinational technology companies in the Republic of Bulgaria, which are a key factor and carrier of modern means and resources at a world level, in order to ensure a contribution to the development of professional competencies and capacity, accelerated implementation of a sharing mechanism, and their inclusion in the process of developing the National Cybersecurity System, including for increasing the overall security of the Internet space in the country, support for small and medium-sized businesses and the Internet community, in national and international centers for

competence.

6.3. Awareness, education and training • **Engaging all**

stakeholders in raising general awareness and understanding of the possible direct and indirect consequences of cyber impacts – including **cyber hygiene and cybersecurity requirements** in all programs to stimulate the development of the digital economy, civil information society, e-governance, technologies and innovations to enhance **cyber culture** and the responsible use of digital information exchange, provision and use of electronic services throughout the supply chain and the common and shared responsibility for cyber hygiene – effective use of **information sharing mechanisms and platforms;**

• Adding aspects of cybersecurity and responsible and safe use of the Internet and new technological challenges (artificial intelligence, blockchain, quantum computing) to **primary and secondary education** programs –

effective linking with the acquisition of ICT skills and computer literacy, the use of electronic content and forms of learning, combination with extracurricular and game-based forms of learning, strengthening the interaction and engagement of industry, society and family;

• Supplementing and developing **pedagogical programs and training for teachers and lecturers** at all levels, including elements of cybersecurity to educate students in the responsible use of ICT and the Internet;

• Updating and modernizing programs in **vocational and university education** in two main areas:

ÿ creating specialists for ICT, the software and technology industry, and in the various fields of MIS and cybersecurity – meeting the requirements for the design and development of cyber-secure and resilient information systems
systems (security, methods and principles for "secure coding", risk assessment, standards and methods);
ÿ building leaders of digitalization and
personnel for the developing digital economy and smart specialization of Bulgaria, in accordance with new technological trends and the requirements for cyber resilience of dependent business models, productions and services from digital technologies;

o Significant increase (by over 50%) in the number of graduates and graduates
work in the Republic of Bulgaria of specialists in digitalization, including cybersecurity; o Creation of master's programs for the
training of information managers and cyber resilience managers, digitalization managers for the administration, the security sector and industry;

• Effective use of forms of **continuing education, additional qualification and retraining** at all levels to supplement and update competencies in the field of cybersecurity and the use of ICT in connection with the rapid development of technologies and platforms and the resulting new responsibilities and threats, functional and thematic qualification in accordance with established standards and certification by creating certification programs for employees in the administration, the security sector and the academic sector;

• Organizing specific sectoral and cross-sectoral **simulations, exercises or drills** with the aim of increasing the knowledge and skills of employees in the administrations of administrative bodies to deal with cyber incidents and cyber attacks, within the scope of national and international exercises or drills.

• Development and use of modern methods and tools for accessible, attractive and engaging learning at all levels – innovative use of all media channels and continuously developing forms, social networks, game elements and forms of social and collective engagement, constantly operating programs and campaigns and inclusion in global and European initiatives (such as Cybersecurity Month78, competitions, “hackathons”).

• Support for conducting a National Campaign for Digital Transformation within the framework of the strategy “Digital Transformation of Bulgaria for the period 2020 -

78 European Cyber Security Awareness Month (October)
US: https://en.wikipedia.org/wiki/National_Cyber_Security_Awareness_Month ENISA:
https://cybersecuritymonth.eu/

2030”79 , reaching all levels of society and in the context of the development of the digital decade in the EU.

7. International interaction, cyber diplomacy

Goals:

Objective 1: *Bulgaria will play an active role in international cooperation in the field of cybersecurity at the European and global levels. It will contribute to the formation of international strategies, the development of legally binding regulations, criminal prosecution, information exchange, participation in international exercises with a focus on cybersecurity and the development of joint cooperation projects within NATO, the EU, the UN and the OSCE.*

Goal 2: *Bulgaria will continue to fulfill its alliance commitments within NATO. in the field of cyber defense and will actively participate in the implementation of the Memorandum of Understanding on Cyber Defense, the Cyber Defense Industry Cooperation Initiative approved during the Alliance Summit in Wales, as well as the NATO Cyber Defense Commitment from the 2016 Summit and the decisions taken at the NATO Summit in Brussels in 2018.*

Objective 3: *Bulgaria's commitments within the EU are linked to the priorities set out in fundamental documents such as the European Cybersecurity Strategy, the Framework for a Joint EU Diplomatic Response to Malicious Acts in Cyberspace and the European Cyber Defence Policy Framework. The main objective is to build guaranteed maximum secure access to the internet. In order to improve national capabilities and address cyber threats, Bulgaria should actively cooperate with EU bodies dealing with cybersecurity issues (EU Cybersecurity Agency, Europol, European Defence Agency), and develop regional and bilateral cooperation and interaction.*

Priority areas of action

7.1. Cyberdiplomacy

An important element of Bulgaria’s commitments to ensuring a free and secure cyberspace is its work in the field of cyber diplomacy. The conclusions adopted by the Council on general issues on cyber diplomacy80 define as key the further development of **a common and comprehensive European approach to cyber diplomacy.** The framework for a joint diplomatic response (the so-called cyber diplomacy toolbox) enables the EU and its Member States to use all measures of the Common Foreign and Security Policy (CFSP), including, where necessary, restrictive measures, to prevent, deter, deter and respond to malicious actions in cyberspace against the integrity and security of the EU and its Member States. The EU

79 Adopted by Decision of the Council of Ministers No. 493/17.07.20,

80 See 6122/15 of 11.02.2015 Annex: Council Conclusions on Cyber Diplomacy

and Member States should work together to achieve the strategic objectives set out in the Conclusions:

- Respect and promote respect for **human rights in cyberspace** (providing assistance to victims of internet crimes, fighting organised crime, conducting investigations and preserving electronic evidence, ensuring safe and affordable access for all citizens, promoting the implementation and better use of the European Guidelines on Freedom of Expression, including online, and the European Guidelines for Human Rights Defenders);

- Norms of conduct and **application of the norms of international law in the field of international security** (achieving agreement and a common vision for the application of existing international law in cyberspace, upholding the position that international law is also applicable on the Internet);

- Internet governance (as an integral part of the EU's overall and comprehensive approach to cyber diplomacy);
- Strengthening **the competitiveness and prosperity of the EU** (with a focus on further promoting the **European Digital Single Market** and strengthening IT security, including the digital economy in the national agenda, close cooperation with international partners on data protection, harmonizing standards and building trust with third countries);

- Cyber capacity building and development - developing a common approach to cyber capacity building and making it an integral part of a broader, global approach in all cyber areas, including through close interaction with relevant EU bodies, using various financial programs and instruments for sustainable cyber capacity building and developing cyber resilience;

- Strategic cooperation with key partners and international organizations to implement a coherent, effective and coordinated cybersecurity policy with a view to avoiding duplication of activities and initiatives, implementing close cooperation with international organizations working in the field of cybersecurity;

- Activation and development of cooperation within the framework of the Organization for Security and Cooperation in Europe (OSCE)81, with initiatives, programs and activities of the UN, international organizations and networks.

7.2 Interaction at technical, operational and strategic levels

- Establishing and updating the regulatory framework and international agreements for effective implementation of operational interaction between the bodies and structures of the National Cybersecurity System and the National Cybersecurity Commission with the relevant bodies and institutions from the EU, NATO and on a bilateral basis with partner countries for the development of joint capabilities;

- Institutionalize and negotiate the framework for interaction in relation to information sharing platforms, both state and mixed

81 Implementation of the OSCE PA Decisions on Confidence-Building Measures in Cyberspace (PC Decisions 1039, 1202).

public-private level in sectors and areas related to CI, CCII, strategic resources, as well as the new developing sensitive areas of Internet-based services (e-commerce, healthcare, finance, etc.);

- Development and participation in regional initiatives and projects in the field of cybersecurity, cyber resilience and protection of CI and shared cross-border assets and activities;

- Ensuring the regulatory framework and arrangements for conducting international (including regional) joint exercises and tests, sharing resources, capacity and information.

8. Implementation, control and update

The updated National Cybersecurity Strategy has a horizon until 2023. It has been developed based on a review and assessment of the National Cybersecurity Strategy "Cyber Resilient Bulgaria 2020" by an interdepartmental expert working group appointed by the Prime Minister, including representatives of all stakeholders. The Cybersecurity Council will propose it for adoption to the Council of Ministers of the Republic of Bulgaria.

For the implementation of the Strategy , **a Roadmap** will be developed , which will be adopted by the Council of Ministers within six months to 6 months after the adoption of the Strategy. All stakeholders will be involved in prioritizing the projects and initiatives included in the roadmap - state, business and industry, academic, research and non-governmental organizations, taking into account the necessary funding by organizations and centrally for the implementation of the Strategy. Implementation is the responsibility of the designated leading institutions and organizations, and the implementation of all priority actions and measures will be based on the principles and methods of project and program management, evaluated on the basis of key indicators and oriented towards results. Specialized national and regional exercises and tests will be organized and conducted to validate the results of the implementation of the projects, as well as participation in international and partnership ones will be increased.

The coordination of the implementation of the Strategy and the Roadmap is carried out by the National Cybersecurity Coordinator, in his capacity as Secretary of the Cybersecurity Council. To assess the progress of implementation, the results achieved in individual areas, the implementation of priorities and action guidelines, an annual report is prepared, and if necessary, an update of the Strategy and, accordingly, the Roadmap is proposed. To increase the awareness and commitment of all stakeholders and groups

of the population and business, as well as for partner countries and structures, an adequate presentation of the Strategy, the Roadmap in form and content should be prepared and their periodic updating should be carried out using accessible information, graphic, media and interactive means.

The Strategy, together with the necessary references and explanations, is provided to all EU Member States and NATO allies, as well as to other countries and organizations based on bilateral agreements and relationships in the field of cybersecurity (OSCE, UN, ITU, countries in the region, etc.). The targeted measures and

Activities are coordinated and updated with the relevant bodies and partner organizations from the EU and NATO, and the necessary additional arrangements are made for the implementation of the identified joint tasks and activities, as well as participation in joint programs and initiatives.

The development of an entirely new national strategic document will begin after the entry into force of the new EU legislation82 83 . and when taken under attention The Communication from the EC to the European Parliament and the Council on an EU Cybersecurity Strategy for the Digital Decade84 .

The commitment of the Member States to adopt new National Cybersecurity Strategies stems from the requirements set out in the relevant directive85 for their content and scope, as well as for the periodic assessment of implementation, at least every four years, based on key indicators and, if necessary, the adoption of relevant amendments and supplements to them.

82 COM(2020) 823 final /16.12.2020 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity

83 COM(2020) 829 final /16.12.2020 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities

84 Joint communication to the European parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade

85 DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity

Appendix:Dictionary

Definitions86

Computer Security Incident Response Team (CSIRT)
Computer emergency response team/CERT. - a structure that studies vulnerabilities in cyberspace and assists victims of hacker attacks, provides 24/7 services, shares information to enhance cybersecurity, and coordinates responses to cybersecurity threats.

Threat - a fact or event with the potential to cause serious harm to the activities of organizations, assets, people or even the state, through unauthorized access, destruction, disclosure and modification of data, and/or denial of services. (ISO 27000: potential cause of an unwanted incident that can cause harm to a system or organization).

Cybersecurity - a state is a state of society and the state, in which, through the implementation of a complex of measures and actions in cyberspace, it is protected from threats related to its independent networks and information infrastructure or which may disrupt their operation. Cybersecurity includes network and information security, counteraction to cybercrime and cyber defense /According to Art. 2, para. 1 and para. 2, of the ZCS/

Cyberspace – a global network of computer processing systems, electronic communications networks, computer programs and data. /According to item 17 of the Civil Code of the Republic of Bulgaria/

Cybercrime – a socially dangerous act /action or inaction/, committed culpably and declared punishable by law, directed at or committed in cyberspace.

Cybercrime (EU) - covers traditional crimes (e.g. fraud, forgery and identity theft), content-related crimes (e.g. online distribution of child pornography or incitement to racial hatred), and crimes that are only possible with computers and information systems (e.g. attacks against information systems, denial of service and malware).

Cyberattack – an attempt to destroy, disclose, modify, disable, steal or obtain unauthorized access to/or unauthorized use of an information asset. /According to item 10 of the Additional Provisions of the Civil Code/

86 Note: According to consultation with the Institute of Bulgarian Language of the Bulgarian Academy of Sciences, the combined terms used related to "cyber" can be written separately or together (merged). For unity in this document and adopted standard of separate writing, and formation of corresponding abbreviations.

(NATO) – Actions taken to disrupt, reject, degrade, or destroy information contained in a computer and/or computer network, as well as the computers and/or computer networks themselves.

(ISO 27000) - Attempt to destroy, disclose, alter, disable, steal
obtaining unauthorized access to or making unauthorized use of
of an asset.

Cyberwarfare - Cyberwarfare is any politically motivated conflict in cyberspace characterized by cyberattacks against the enemy's computer and information systems.

Cyberwarfare (2) - Military operations conducted in virtual space using information technology tools and methods. In a broader sense, this is the support of military operations conducted in traditional operational spaces - land, sea, air and space - through actions carried out

in virtual space.

Cyber incident – an event or series of unwanted or unexpected events related to cybersecurity that are likely to compromise activities and threaten information security. /According to item 12 of the Civil Code of the Republic of Bulgaria/

(NATO) - an unexpected event in cyberspace that, with or without criminal intent, could alter cybersecurity by actually or potentially compromising the confidentiality, integrity, or availability of an information system or the information the system processes, stores,

or conveys, a violation or potential violation of security policies,
security procedures or acceptable use policies.

(ISO 27000) – An event or series of unwanted or unexpected events related to cybersecurity that has a high probability of causing a compromise of activities and threatening the security of information

Cyber crisis – a serious threat to the functioning of basic structures of the state and the economy, and/or fundamental values and norms of society, caused by malicious actions in cyberspace, which, due to lack of time and in uncertain circumstances, requires making vital decisions on

national level.

Cyber defense – a complex of measures and capabilities for protection and active counteraction to cyberattacks and hybrid impacts on communication and information systems and defense and armed forces management systems,

as well as on the systems for governing the country in times of emergency, martial law or war and on strategic objects that are important for national security. /According to item 16 of the Draft Law of the Civil Code/

Cyber reserve – an additional resource of experts in the field of cybersecurity, information protection and information technologies, with competencies related to ensuring the protection and sustainability of communication and information systems. /According to item 18 of the Supplementary Provisions of the Civil Code/

Critical infrastructure – strategic objects and activities of importance for national security - According to Art. 1, para. 1 of PMS No. 181 of July 20, 2009, strategic objects and activities of importance for national security are defined in a single list and are part of the critical infrastructure. The legal definition of CI is contained in §1, item 15 of the Draft Law of the Disaster Protection Act: *"A system or parts thereof that are of fundamental importance for maintaining vital public functions, health, safety, security, economic or social well-being of the population and whose disruption or destruction would have significant negative consequences for the Republic of Bulgaria as a result of the impossibility of maintaining these functions."*

Critical communication and information infrastructure - systems, services, networks and infrastructures that are a vital part of the national economy and society and provide important goods and services, the destructive impact on which could have a serious impact on vital functions of society. Critical information infrastructure are both the networks, channels and the systems for their management and maintenance.

Network and information security – the ability of networks and information systems to withstand a certain level of impact,
negatively affecting the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the related services offered by or accessible through these networks and information systems. /According to Art. 2, para. 3 of the ZCS/

Breach - an unauthorized action that overcomes security mechanisms
of the systems.

National Computer Security Incident Response Team –
structure within the SAEU, performing functions defined in Art. 19 of the ZCS

Risk – the potential possibility of a given threat being realized by exploiting the vulnerability of information assets to cause harm. /According to item 30 of the DD of the ZCS/

Sectoral Computer Security Incident Response Team –
structure under an administrative body under Art. 16, para. 1 of the ZCS, performing functions defined in Art. 18 of this law

Resilience (NIST) – ability, property (of the organization) to quickly
to adapt and recover from known or unknown environmental changes

through comprehensive and consistent implementation of risk management, emergency management and business continuity planning.

Vulnerability - instability of the information system, internal control and security procedures and their implementation, which can be used to have a destructive impact on the system. /According to item 34 of the Additional Provisions of the Civil Code/

Hybrid threat87 – an identified intent and capability by a state or non-state actor that may employ a hybrid strategy. It is assessed that in order to employ a hybrid strategy, a non-state actor has the ability to implement

all, or almost all, elements of power characteristic rather of a sovereign country.

Hybrid warfare model – used to refer to modern conflicts that combine conventional and unconventional actions, cyberattacks, psychological and economic impact, disinformation campaigns, infiltration of the information environment, creating panic, financing of deliberately created political entities in order to change the foreign policy line of the targeted adversaries and other actions to achieve political and strategic goals. The hybrid model is a specific manifestation of a given hybrid strategy used by a specific adversary. Each hybrid strategy is unique, therefore each response must be adapted to its specificities.

Digital dependency – critical dependence of the performance of the core functions and activities of institutions, organizations, businesses and society as a whole on ICT.

Digital infrastructure – infrastructure that includes TOI, DNS service providers and top-level domain name registries. /According to item 36 of the Additional Provisions of the ZCS/

Abbreviations

ICT	Information and communication technologies
DOG	Information technology
SPEAK	Qualified electronic signature
WHO	Critical infrastructure
KIN	Confidentiality, integrity, availability (information security)
WHO	Communication and information systems
CCII	Critical communication and information infrastructure
MERGE	Interdepartmental Expert Working Group

87 National "Strategy for Countering the Hybrid Model of Warfare"

MIS	Network and information security
SMEs	Small and medium-sized enterprises
NCCOMKS	National Cybersecurity Coordination and Organizational Network
NSC	National Situation Center
NXC	National Cyber Situation Center
NGO	Non-governmental organization
PPP	Public-private partnership
APT	Advanced Persistent Threats
CIA	Confidentiality, Integrity, Availability (CIS - information security)
CERT	Computer Emergency Response Team (ÿÿÿÿ Computer Emergency Readiness Team)
CSIRT	Computer Security Incident Response Team
ICS	Industrial Control Systems
IoT	Internet of Things (Internet connected devices, Industrial internet)
THAT	International Telecommunications Union
ISAC/ISAO	Information Sharing and Analysis Center/Organization
MIL CIRC	Military Computer Incident Response Center
NCIRC	NATO Computer Incident Response Capability
NIS	Network and Information Security
SCADA	Supervisory Control And Data Acquisition

Organizations, institutions

DAEU	State Agency for Electronic Governance
ACCOUNT	State Agency for National Security
IN	State Intelligence Agency
GIVEN	State Agency "Technical Operations"
SCIS	State Commission for Information Security
EC	European Commission
EU	European Union
ESOS	European interoperability strategy
Cattle	Communications Regulatory Commission
Ministry of Interior	Ministry of Interior
Ministry of Foreign Affairs	Ministry of Foreign Affairs
MON	Ministry of Education and Science
MS	Council of Ministers
MTITC	Ministry of Transport, Information Technology and Communications

NATO / NATO North Atlantic Treaty Organization/North Atlantic Treaty Organization	
NCCS	National Cybersecurity Coordinator
UN	United Nations
OP	Operational program
RB	Republic of Bulgaria
Security Council under the Council of Ministers Security Council under the Council of Ministers	
SKS	Cybersecurity Council
EDA / ÿÿÿ European Defense Agency / European Defense Agency	
ENISA	European Union Network and Information Security Agency
ICANN	Internet Corporation for Assigned Names and Numbers
NCI Agency NATO Communications and Information Agency	
NIST	US National Institute of Standards & Technology/