Republic of Bulgaria

Council of Ministers

National Cyber Security Strategy
Cyber Resilient Bulgaria 2020

www.cyberBG.eu
Adopted on July 13, 2016


Krasimir Simonski
Executive Director
EA ECNIS, MTITC
ksimonski@esmis.government.bg

Dr. George Sharkov
National Cybersecurity Coordinator
Security Council, Council of Ministers
g.sharkov@mod.bg
g.sharkov@government.bg
National Cyber Security & Resilience: A multi stakeholder engagement

www.cyberBG.eu

Civil society & Citizens

State

Business & Industry, Academia

National strategies
USA, UK, Netherlands, Austria, Germany, Finland, ...
Cyber Resilience Context

Unknown unknowns
unforeseeable, unpredictable

Known unknowns
non-CIA complex threats, APTs

Known knowns
CIA triad threats

Cyber security

Cyber resilience

Cyber resilience context.
CIA: Confidentiality, Integrity, Availability

Bulgarian context: How to protect against the unknown?

• Risk environment will NOT contract—number of risks and complexity will increase
• Organizations must get better at “surviving” in uncertainty
• Knowledge and awareness of risk issues must be pervasive throughout the organizations
• Traditional tools, techniques, and methods may not work in this environment
• Existing organizational structures and governance model may not be agile enough to adapt
Vision: Cyber Resilient Bulgaria 2020

3 phases for 5 years:

Phase 1: **Cyber secure institutions**
- National coordination platform
- Engaging all stakeholders
- Inventory & Risk assessment

Phase 2: **Cyber secure society**
- From capacity to capabilities
- International coordination networks
- Resilient organizations (by design)

Phase 3: **Cyber resilient organizations and society**
- Effective collaboration at national level
- International joint capabilities – NATO/EU
- Specialization and leadership

Credit: Eurocontrol: Manual for National ATM Security Oversight
Resilience strategy “translated”:
9 fields of action, 18 goals and > 100 measures

1. **Establish National Cyber Security and Resilience System**: governance, situational awareness (“cyber picture”), coordinated response & prevention

2. **Network and information security (NIS) – the foundation for cyber resiliency**: minimal NIS requirements, specific for government and state administration CIS, institutions, CI, private sector engagement (ISP), CERTs capabilities (aligned with the EU NIS Directive)

3. **Improving the protection and sustainability of digitally dependent critical infrastructures**: state-operators collaboration, system modernization vs. patching, scope of CI measures (new areas) – essential services (NIS Directive)

4. **Better cooperation between government-economy-citizens**: information sharing platforms, ISACs/ISAOs and CERTs, NGOs, PPP, industrial and technology capacity development

5. **Legal and regulatory framework**: harmonization of legal, regulations and standardization, self regulation

6. **Cyber crime counter fighting**: capacity development (organizational and administrative), law enforcement basis update, coordination, prevention

7. **Cyber Defense**: defense and armed forces CIS protection, national security (incl. counter terrorism, CI protection, hybrid threats and crisis)

8. **Awareness, education and innovation**

9. **International cooperation**: EU, NATO, OSCE, UN, ITU, ICANN, and regional, cross border
Collective engagement: Public-Private Partnerships

The Public-Private Partnership (PPP) on cybersecurity

To strengthen EU’s cybersecurity industry, the European Commission will establish a contractual Public-Private Partnership (PPP) on cybersecurity, as envisaged in the Digital Single Market Strategy.

The European cybersecurity industry by:
- Mobilizing public and private resources to improve Europe’s industrial cybersecurity, innovation and following a jointly-agreed road map
- Engaging and incentivizing states and industrial actors by fostering a cooperative approach and innovation
- Aligning the demand and supply of cybersecurity products and services, and allowing the industry to efficiently scale-up
- Providing visibility to European R&I excellence in cyber security and digital trust

The PPP will build on the Strategic Research Agenda (SRA) in the area of cybersecurity.
National CS Model & System: National Cyber Picture + Coordinated Response

Goals: National & collective security (EU, NATO, regional), Coordinated response, Hybrid threats/warfare

Needs:
• Live Cyber Picture (national situational awareness)
• Continuous monitoring
• Levels of alert – coordinated and adequate response
• Collective and coordinated response
• National CS operational coordination & organization network (NCSCON)
  • State provides the “backbone” (NSCON)
  • Industry, business (ISACs, sector/business CERTs)
  • Citizens, NGOs, society
• Prevention (lessons learned)
• National interoperability – collaborative resilience
• International interoperability – collective engagement and capabilities
Engaging industry & business: ISACs, ISAOs + CERTs/CSIRTs

CERTs + ISAC
Finances
Banks
Insurance
Engaging SMEs & business: Shared (cyber) risk over supply/value chains
Covering new and emerging areas of Digital Dependency: Essential services, Digital Services Providers (NIS Directive), IoT
Cyber Defense: Cyberspace as the 5th Domain: From “defense” to “resilience”
R&D, academia, education:
Incubate resources & Industry Specialization
The “key” keyword: COORDINATION

https://www.us-cert.gov/nccic
Exercises to validate and build capabilities:

Target model: [US] Cyber ShockWave (February 2010)
[BG] Our National Cyber ShockWave-s:
- Transport (27.10.2016)
- Banks (private initiative, Banks ISAC / CIO Club)

“Cyber ShockWave” Exercise Shakes Up the Capital: How Would Our Leaders Respond to an All-Out Cyber Crisis?

A report was released yesterday detailing the fallout of an extraordinary simulated cyber attack scenario, which was orchestrated in Washington DC on February 10, 2010, by a bipartisan group of former senior administration and national security officials.

CNN’s Wolf Blitzer moderated and broadcast a special news program on the “Cyber ShockWave” simulation. The purpose of the exercise was to gain insight into how government officials would respond in the event of a large-scale cyber crisis affecting much of the nation.
“If you are not part of the solution, you must be part of the problem”

Attributed to: Eldridge Clever (1969); African proverb, others