Republic of Bulgaria

Council of Ministers

National Cyber Security Strategy
Cyber Resilient Bulgaria 2020

www.cyberBG.eu

Adopted on July 13, 2016

[ITU , ENISA] Regional Cybersecurity Forum, 29-30.11.2016, Sofia

Krasimir Simonski

Executive Director
EA ECNIS, MTITC

ksimonski@esmis.government.bg

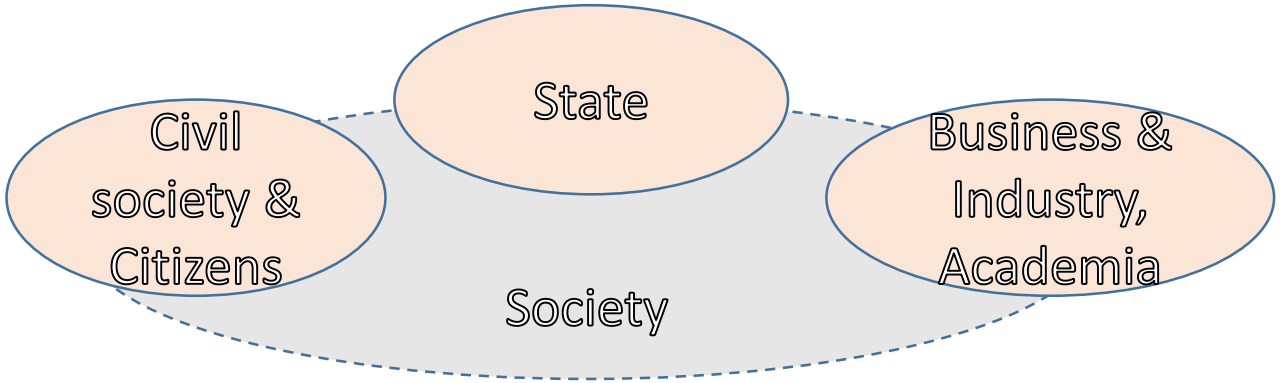
Dr. George Sharkov

National Cybersecurity Coordinator
Security Council, Council of Ministers

g.sharkov@mod.bg
g.sharkov@government.bg

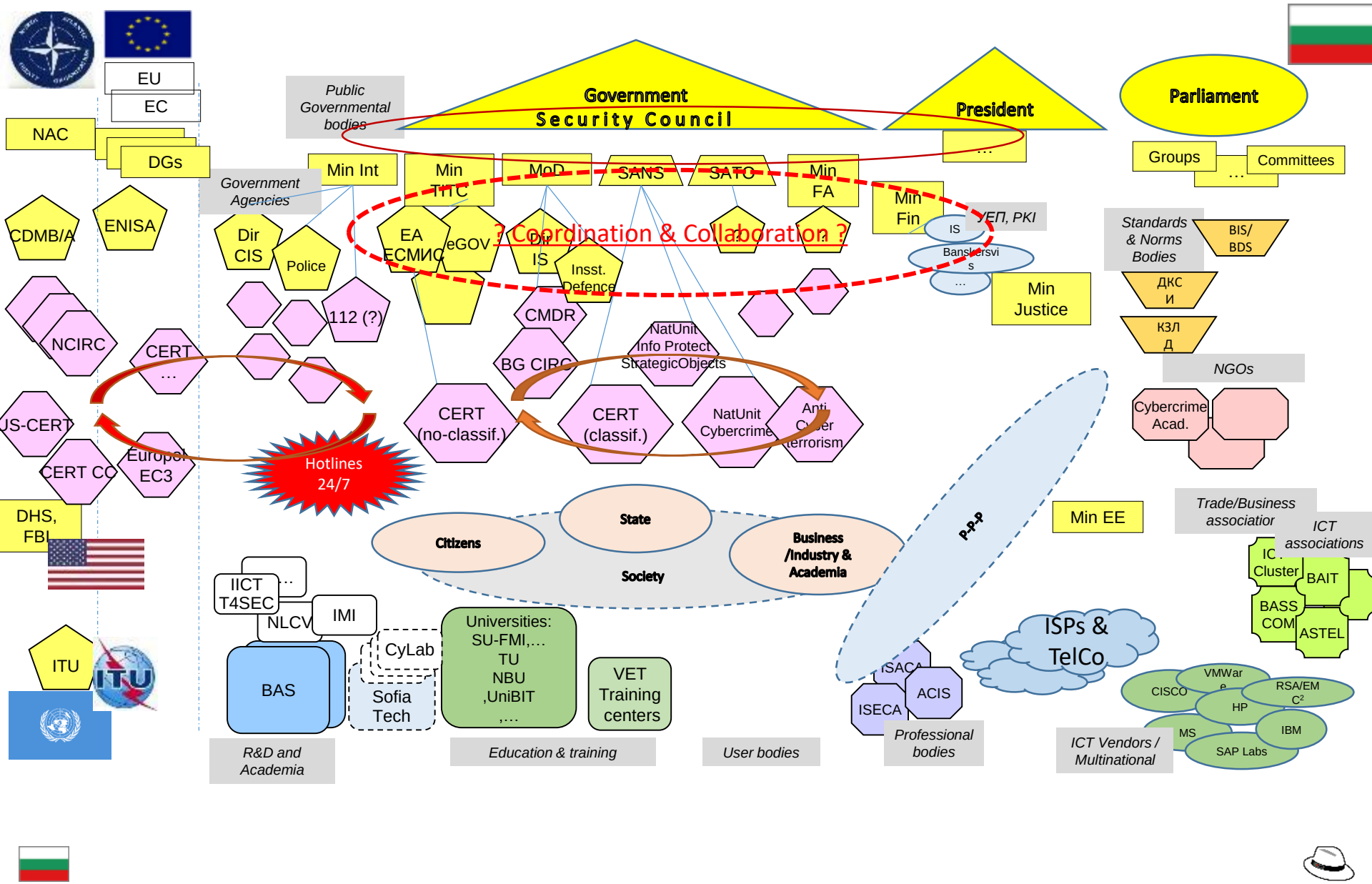
National Cyber Security & Resilience: A multi stakeholder engagement

www.cyberBG.eu

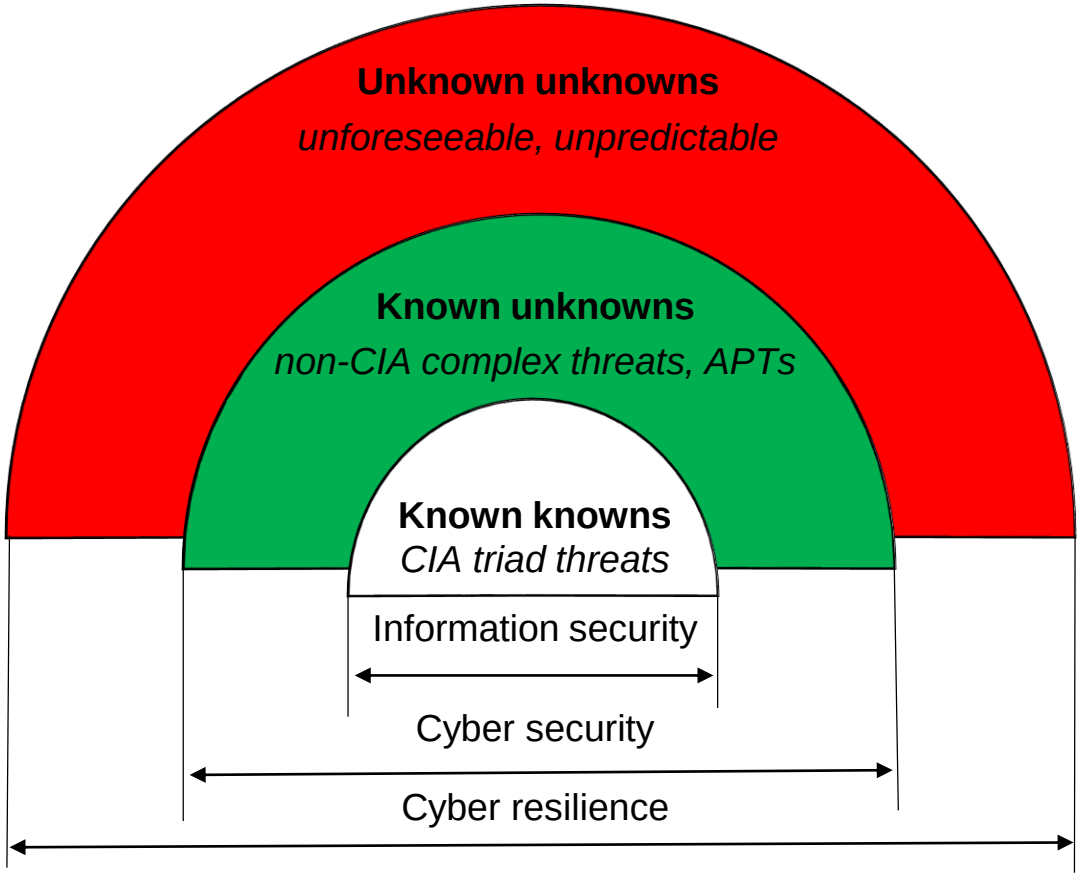


National strategies
USA, UK, Netherlands , Austria, Germany, Finland, …

Bulgaria: Stakeholders Picture



Cyber Resilience Context



Cyber resilience context.

CIA: Confidentiality, Integrity, Availability

Credits: Eurocontrol: Manual for National ATM Security Oversight & Nassim Taleb “Black Swan”

Bulgarian context:
How to protect against the unknown?

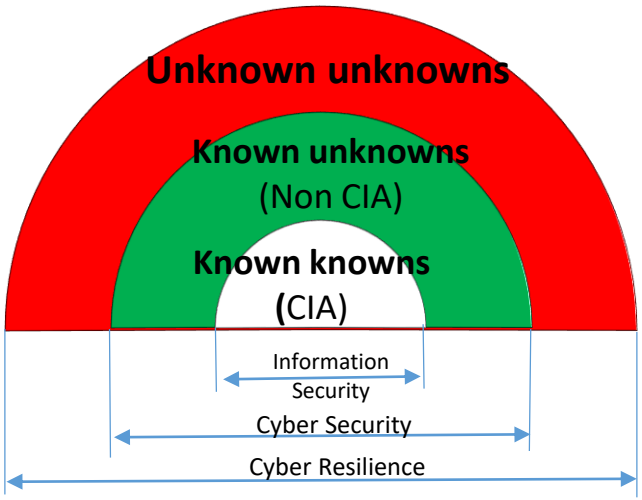
- Risk environment will NOT contract—number of risks and complexity will increase
- Organizations must get better at "surviving" in uncertainty
- Knowledge and awareness of risk issues must be pervasive throughout the organizations
- Traditional tools, techniques, and methods may not work in this environment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

Vision: Cyber Resilient Bulgaria 2020

Initiation
2016 -2017

Growth
2018 - 2019

Maturity & Leadership
2020 +



Credit: Eurocontrol: Manual for National ATM Security Oversight

3 phases for 5 years:

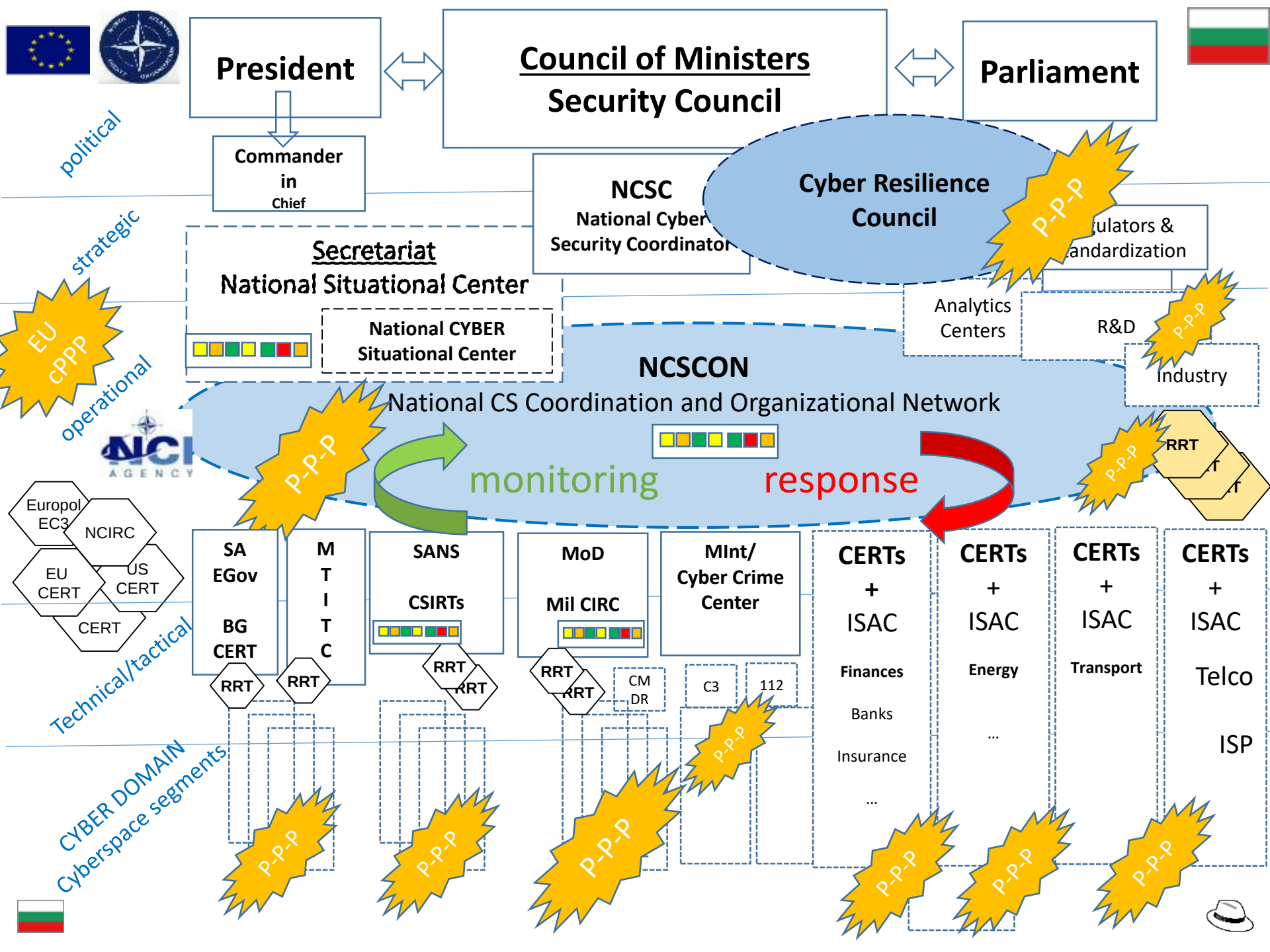
Phase 1: Cyber secure institutions
National coordination platform
Engaging all stakeholders
Inventory & Risk assessment

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

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 Directve)
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


President
Council of Ministers
Security Council
Parliament
political
Commander in Chief
NCSC
National Cyber Security Coordinator
Cyber Resilience Council
P-P-P
ulators & andardization
strategic
Secretariat
National Situational Center
National CYBER Situational Center
Analytics Centers
R&D
Industry
EU cPPP
operational
NCSCON
National CS Coordination and Organizational Network
monitoring
response
RRT
Europol EC3
NCIRC
EU CERT
US CERT
CERT
SA EGov
BG CERT
MITIC
SANS
CSIRTs
MoD
Mil CIRC
MInt/ Cyber Crime Center
CERTs + ISAC
Finances
Banks
Insurance
...
Energy
Transport
Telco
ISP
CM DR
C3
112
Technical/tactical
CYBER DOMAIN
Cyberspace segments

Collective engagement:
Public-Private Partnerships

P-P-P

DIGITAL SINGLE MARKET

Digital Economy & Society

European Commission > Cybersecurity industry

The strategy | Economy | Society | Access & connectivity | Research & innovation | DG CONNECT

Society
Skills & Jobs
eHealth and Ageing
Smart living
Digital Inclusion
Public Services
Cybersecurity and privacy
Cybersecurity
Cybersecurity industry
Online privacy
EU Funded Projects
Online trust
Content and media
Emergency and supp
Societal challenges

Cybersecurity industry

Article | Latest

The cybersecurity market, one of the fastest growing markets in the ICT sector, yields huge economic opportunities. Strengt will allow European businesses to seize thes citizens and businesses in the digital world, Single Market Strategy.

The European market supply for ICT security products and services is significantly fragmented, and therefore European companies are often not able to achieve the

The Public-Private Partnership (PPP) on cybersecurity

To strengthen EU's cybersecurity industry, the European Commission will es contractual Public-Private Partnership (PPP) on cybersecurity, as envisaged i Digital Single Market Strategy.

European cybersecurity industry by:

ic resources to improve Europe's indu innovation and following a jointly-agre admap

States and industrial actors by fosterin and innovation

ustry by aligning the demand and supp s, and allowing the industry to efficientl s

20 and maximizing the impact of availa rdination and better focus on a few techn

- providing visibility to European R&I excellence in cyber security and digita

19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

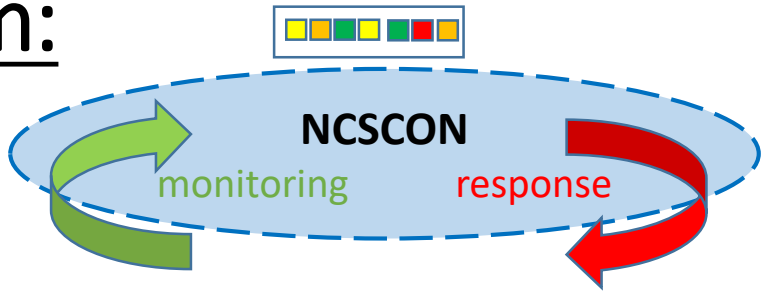
DIRECTIVES

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

National CS Model & System:

National Cyber Picture + Coordinated Response

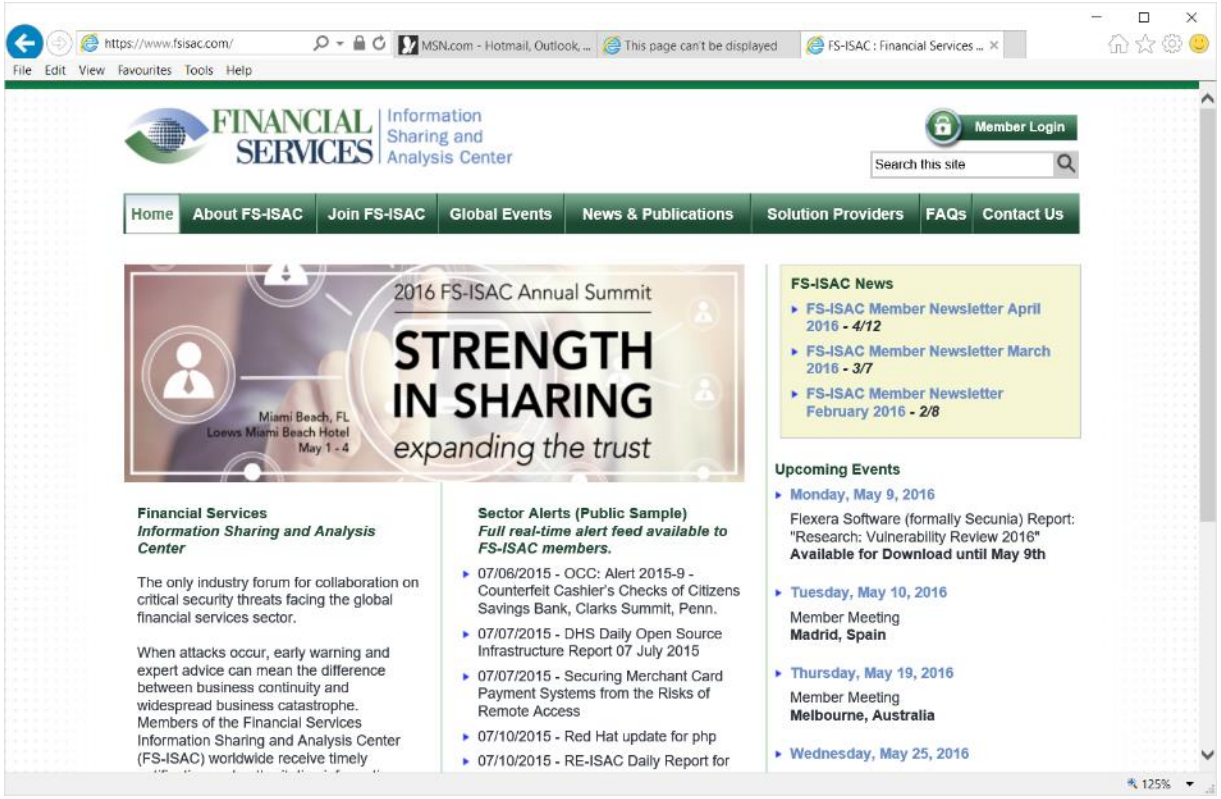


Goals: National & collective security (EU, NATO, regional), Coordinated response, Hybrid threats/warfare

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

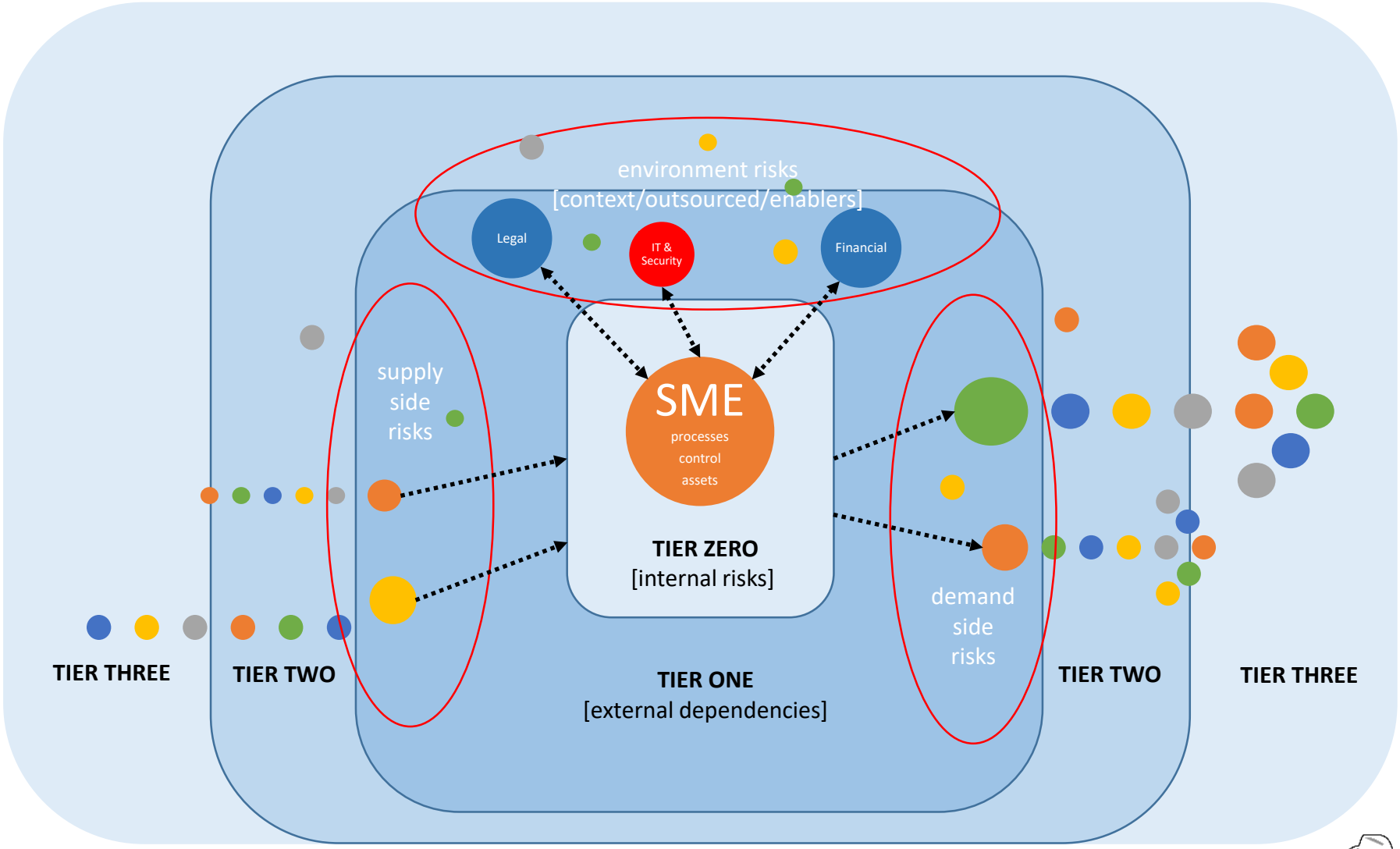
Banks

Insurance

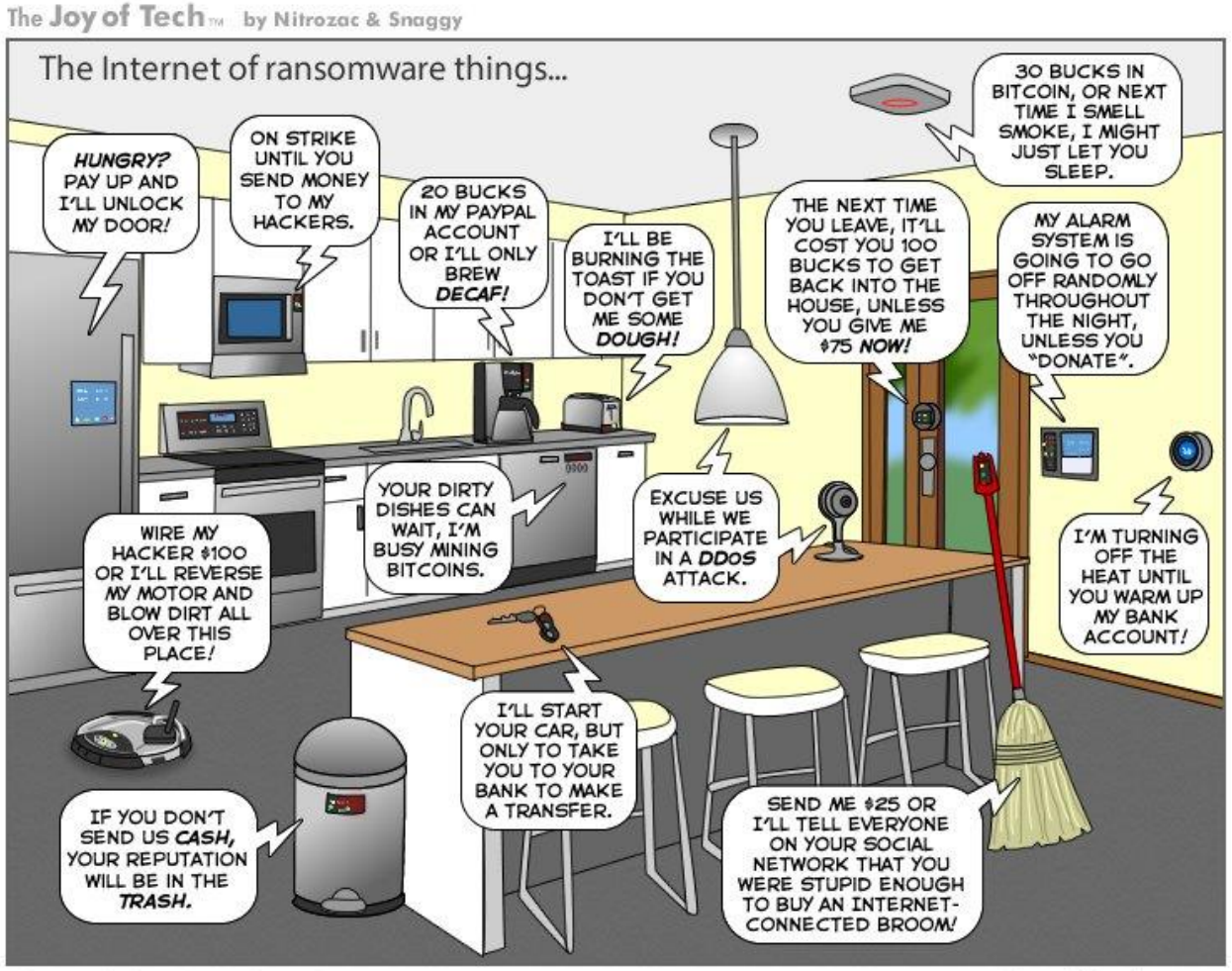
...

P-P-P

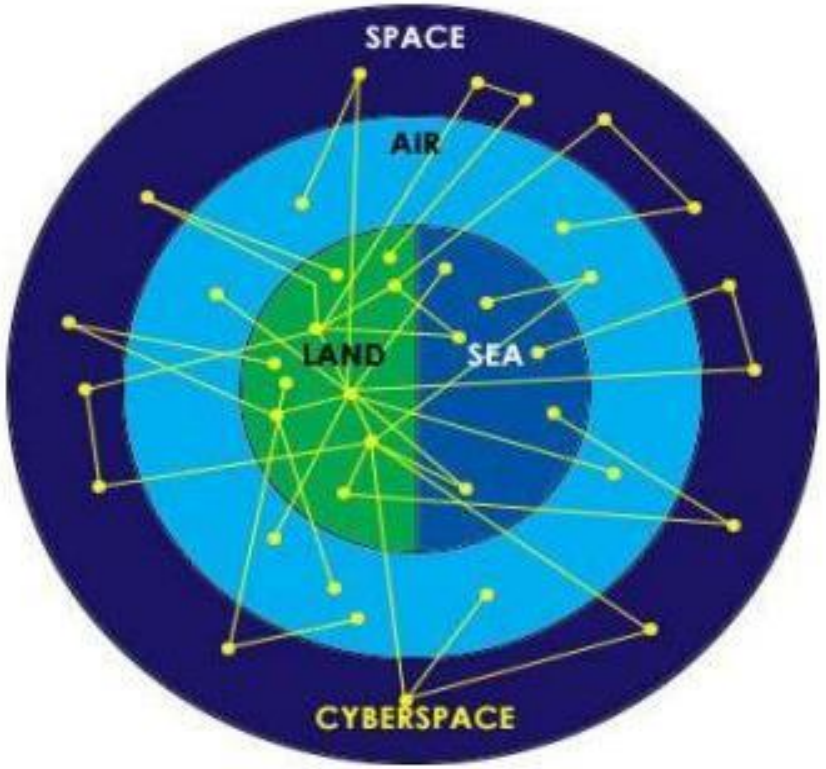
Engaging SMEs & business:
Shared (cyber) risk over supply/value chains



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

National Cyber Situational Center

https://www.us-cert.gov/nccic

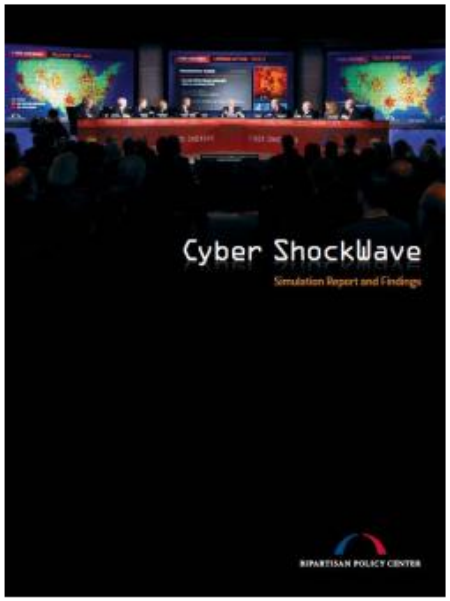
Exercises to validate and build capabilities:

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?

by STEVE.KOVSKY *on* JUNE 29, 2011

A report was released yesterday detailing the fallout of an extraordinary simulated cyber attack scenario, which was orchestrated in Washington DC on February 16, 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.

www.cyberBG.eu

“If you are not part of the solution, you must be part of the problem”

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