ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection

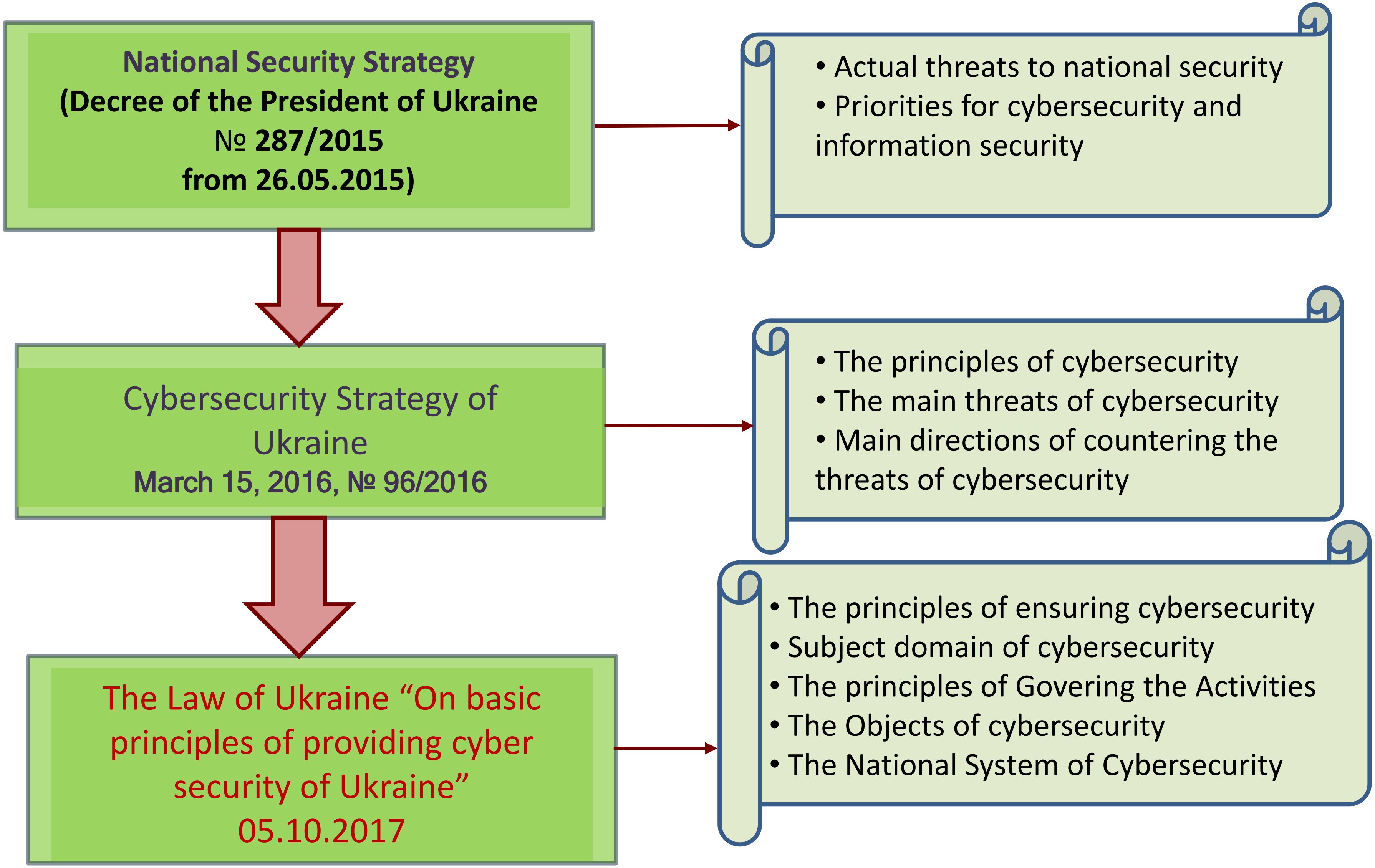
CYBERSECURITY IN UKRAINE: PROBLEM AND PERSPECTIVE

Prof OLEKSANDR POTII

Professor of Department of Information Systems and Technologies Security,
V. N. Karazin Kharkiv National University, JSC Institute of Information Technology, Ukraine

Odessa, Ukraine, April 4-6, 2018

THE REGULAR BASIS OF NATIONAL SYSTEM OF CYBERSECURITY



National Security Strategy
(Decree of the President of Ukraine
№ 287/2015
from 26.05.2015)

- Actual threats to national security
- Priorities for cybersecurity and information security

Cybersecurity Strategy of Ukraine
March 15, 2016, № 96/2016

- The principles of cybersecurity
- The main threats of cybersecurity
- Main directions of countering the threats of cybersecurity

The Law of Ukraine “On basic principles of providing cyber security of Ukraine”
05.10.2017

- The principles of ensuring cybersecurity
- Subject domain of cybersecurity
- The principles of Govering the Activities
- The Objects of cybersecurity
- The National System of Cybersecurity

NATIONAL SECURITY STRATEGY

Actual Threats to National Security

Article 3. The threats of cybersecurity and security information resources of the state.

- the vulnerability of critical infrastructure objects of state information resources to cyber attacks
- -the physical and moral outdated system of state secret and other information with restricted access.

NATIONAL SECURITY STRATEGY

Priorities for cybersecurity and information security in Ukraine (art. 12):

- development of information infrastructure of the state;
- creating a system ensuring cybersecurity;
- CERT network development;
- monitoring cyber space in order to detect present cyber threats and then neutralize them timely ;
- to protect objects of critical infrastructure, government information resources from cyber attacks;
- resection of the software, including outgivings developed in Russia;
- reforming the system of secret information and other undisclosed information, protection of state information resources, e- government systems, technical and cryptographic systems taking into account the experience of NATO and EU countries;
- **creation of a system of training in the field of cybersecurity;**
- development of international cooperation in the field of cybersecurity.

CYBERSECURITY STRATEGY OF UKRAINE

1. The aggression from the Russian Federation:
   - attempts to violate the normal operation of state information recourses;
   - cyber espionage;
   - the use of cyber attacks for political purpose.

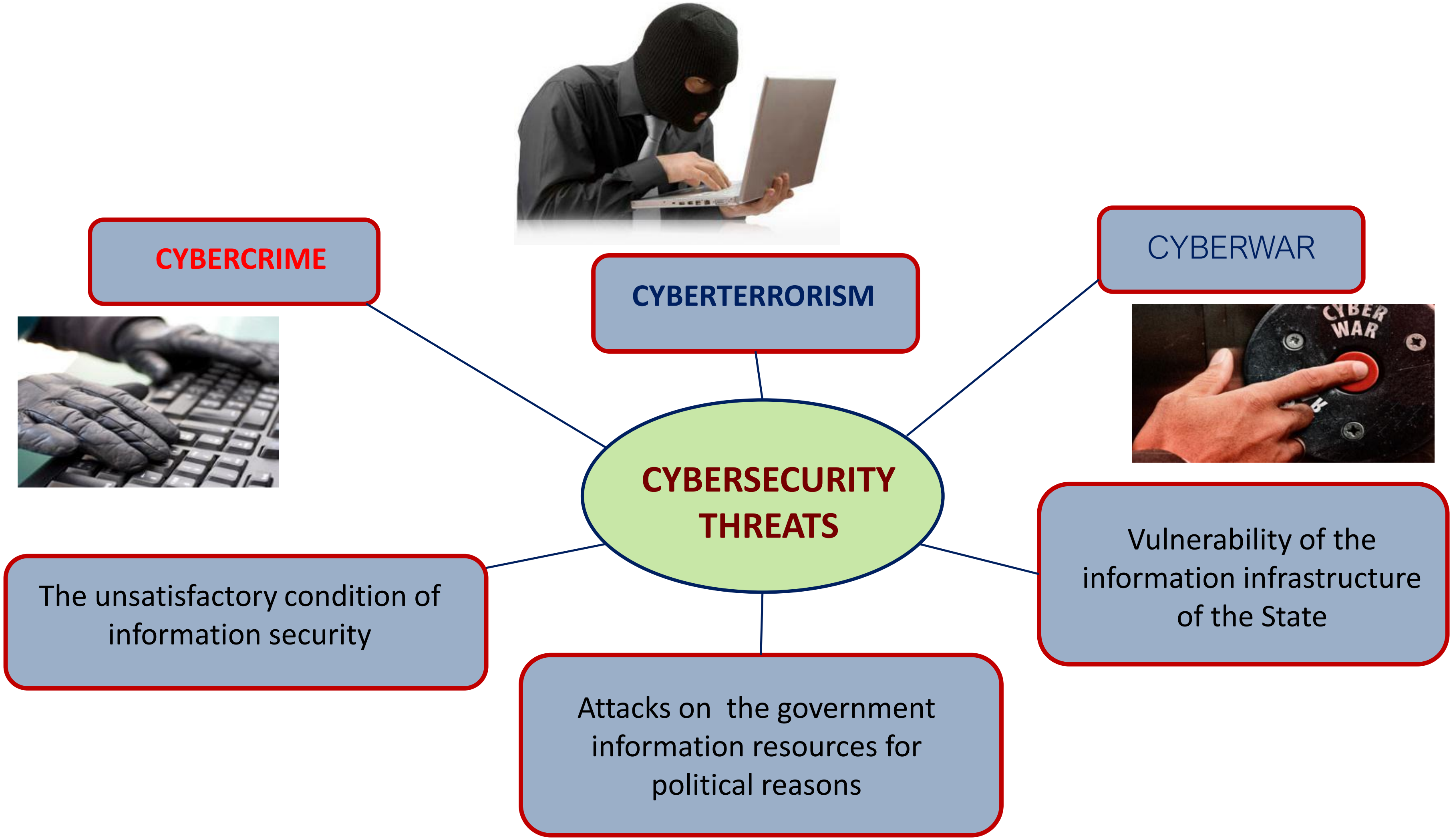
2. The danger of cyber attacks on the implementation of the CII of Ukraine.

3. **International cyber crime.**

4. The increase of internal and external risks in realization of cyber threats.

5. The threats of use of information infrastructure of Ukraine as a transit ground to hide the cyber attacks.

CYBERSECURITY STRATEGY OF UKRAINE



CYBERSECURITY THREATS

CYBERCRIME

CYBERTERRORISM

CYBERWAR

The unsatisfactory condition of information security

Attacks on the government information resources for political reasons

Vulnerability of the information infrastructure of the State

CYBERSECURITY STRATEGY OF UKRAINE

The goal and main principles of activities

THE GOAL: Creation of a modern and flexible national system of cybersecurity to protect the Ukraine's national interests in the information sphere

PRINCIPLES:

1. **The supremacy of law, legality and respect for the rights and freedoms.**
2. **Priority to the protection of personal information and citizens' rights .**
3. An integrated approach to the implementation controls.
4. The priority of preventive protection measures .
5. The inevitability of punishment for the commission of cybercrime.
6. **The interaction of public and private sector in the field of cybersecurity.**
7. Responsibility of critical infrastructure owners for cybersecurity.
8. The effectiveness, comprehensiveness and consistency of security controls.
9. Cooperation at the international level.

CYBERSECURITY STRATEGY OF UKRAINE

Main priorities of the state policy

1. Formation of the regulative framework harmonized with international standards.
2. Organization of effective interaction among state bodies - the subjects of cybersecurity .
3. **Creation of conditions for cooperation between the public and private sectors, citizens and society.**
4. Creating the conditions for cybersecurity information infrastructure.
5. **Development of the training system in the field of cybersecurity.**

THE LAW OF UKRAINE "ON BASIC PRINCIPLES OF PROVIDING CYBER SECURITY OF UKRAINE"

The Structure

Chapter I General Provisions

Art 1. Definition of Terms
Art 2. The legal basis for ensuring cybersecurity of Ukraine

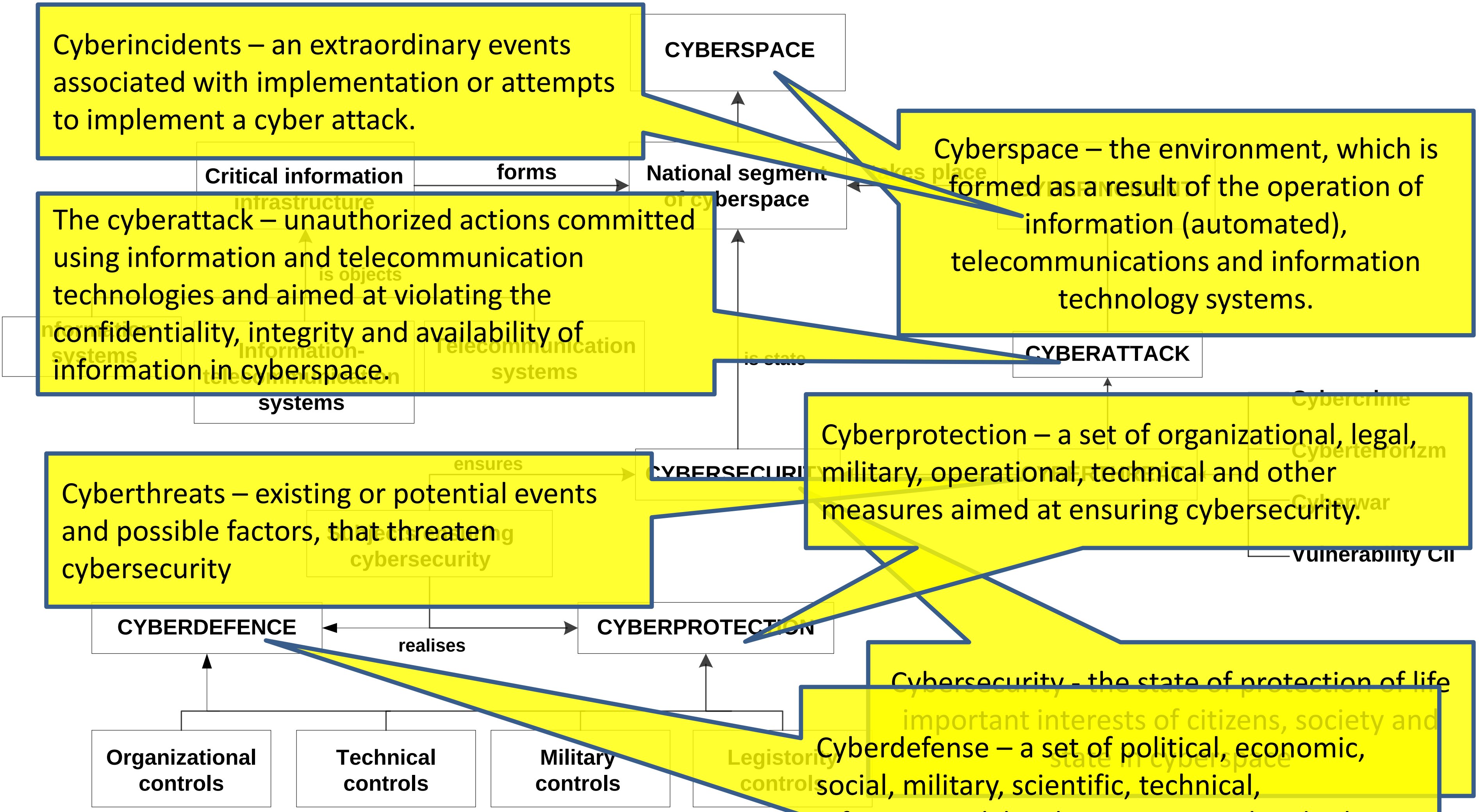
Chapter II Organization foundations ensuring cybersecurity of Ukraine

Art 3. Organizational principles of cybersecurity of Ukraine
Art 4. The main directions of providing cybersecurity of Ukraine
Art 5. Objects of cybersecurity
Art 6. Providing objects cyberprotection of critical information infrastructure
Art 7. The National System of Cybersecurity
Art 8. Authority of subjects providing cybersecurity
Art 9. Interaction of subjects of cybersecurity
Art 10. Promoting cybersecurity of Ukraine
Art 11. Responsibility for violation of legislation of cybersecurity
Art 12. Financial support of cybersecurity of Ukraine

Chapter III International cooperation of Ukraine in the field of cybersecurity

Chapter IV Control over the legality of measures to ensure cybersecurity of Ukraine

SUBJECT FIELD OF CYBERSECURITY



Cyberincidents – an extraordinary events associated with implementation or attempts to implement a cyber attack.

Cyberspace – the environment, which is formed as a result of the operation of information (automated), telecommunications and information technology systems.

The cyberattack – unauthorized actions committed using information and telecommunication technologies and aimed at violating the confidentiality, integrity and availability of information in cyberspace.

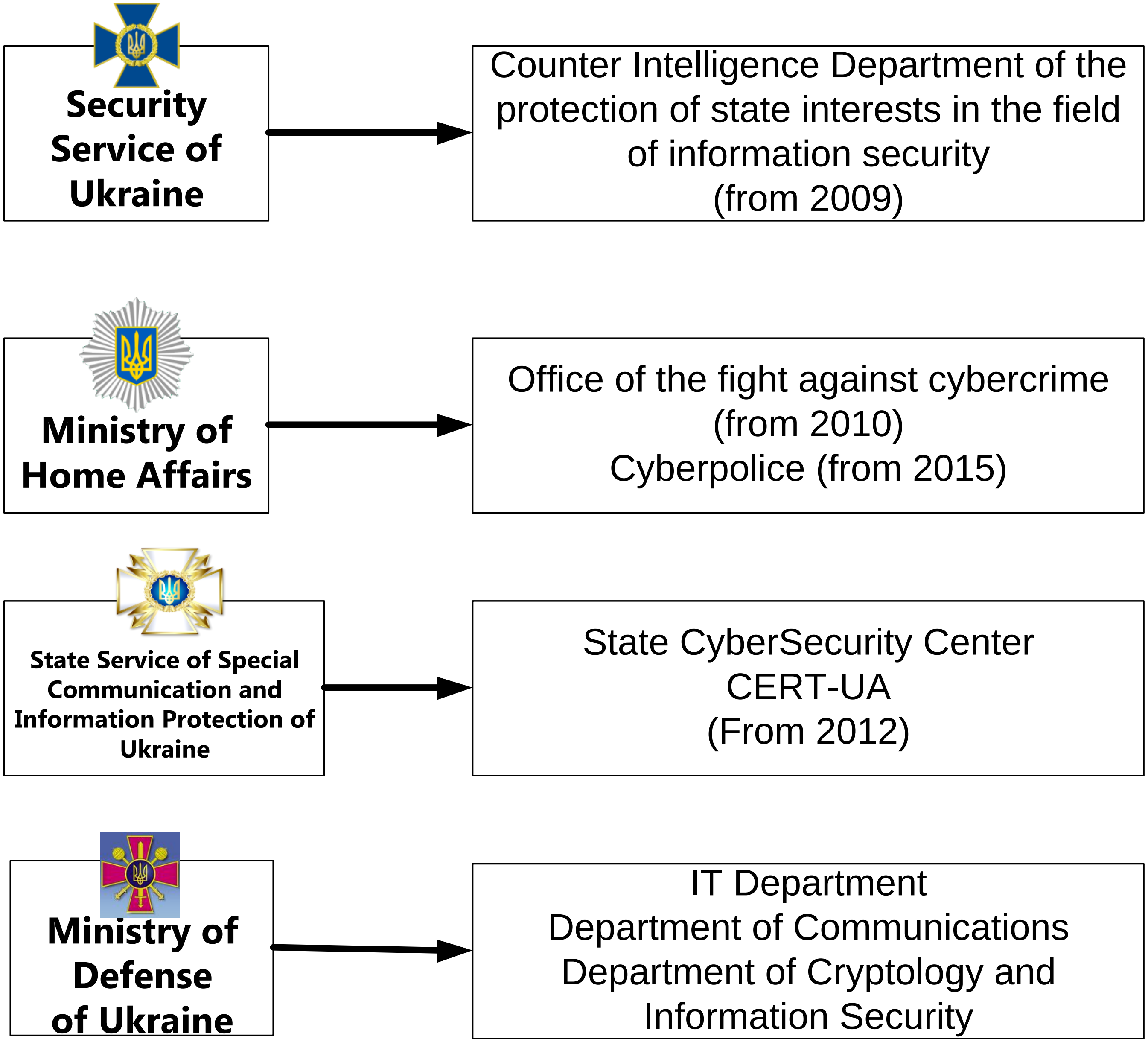
Cyberprotection – a set of organizational, legal, military, operational, technical and other measures aimed at ensuring cybersecurity.

Cyberthreats – existing or potential events and possible factors, that threaten cybersecurity

Cybersecurity - the state of protection of life important interests of citizens, society and state in cyberspace

Cyberdefense – a set of political, economic, social, military, scientific, technical, informational, legal, organizational and other measures to protect the sovereignty of the information and ensure the defense of the state in cyberspace

PRACTICAL MECHANISMS TO ENSURE CYBERSECURITY UKARINE: MODERN-DAY STATE



Security Service of Ukraine

Counter Intelligence Department of the protection of state interests in the field of information security (from 2009)

Ministry of Home Affairs

Office of the fight against cybercrime (from 2010)
Cyberpolice (from 2015)

State Service of Special Communication and Information Protection of Ukraine

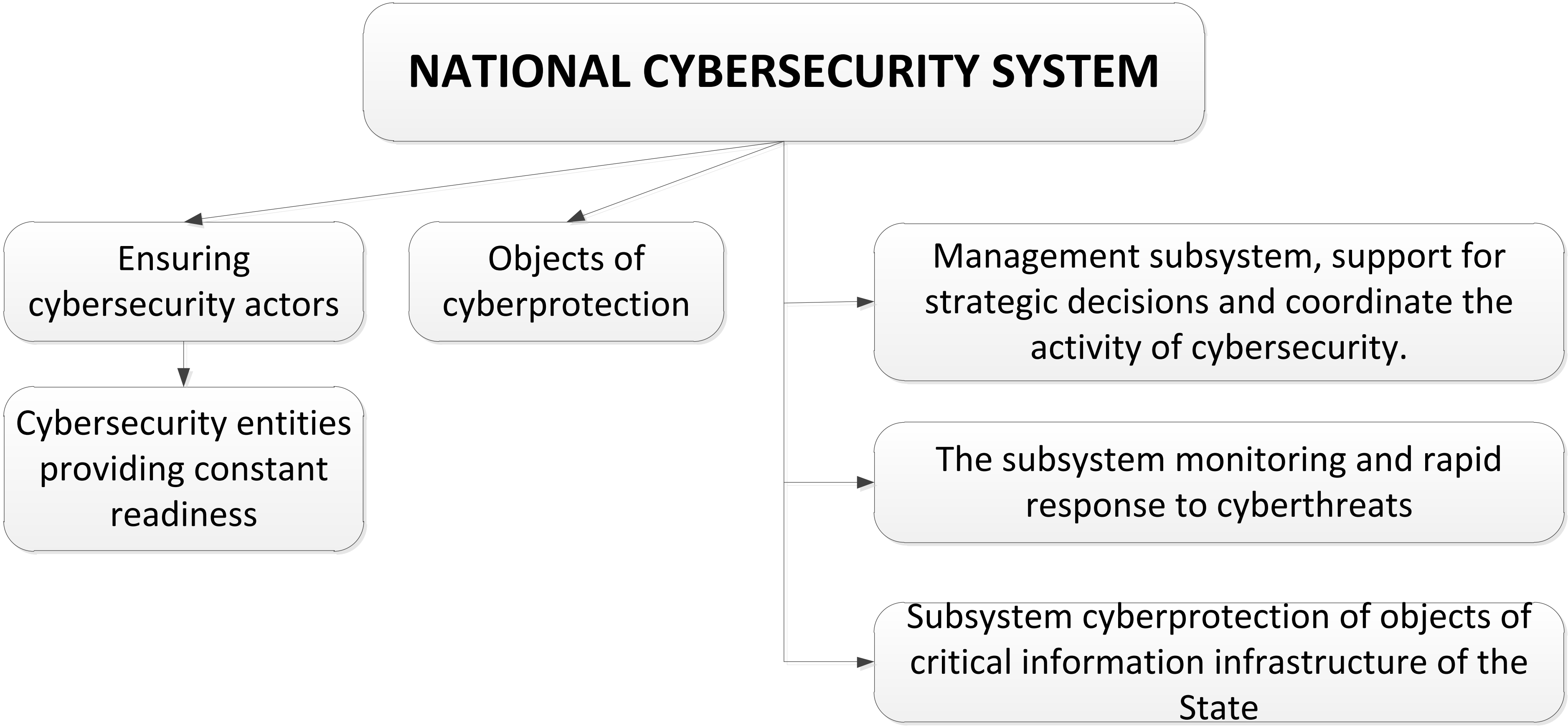
State CyberSecurity Center
CERT-UA
(From 2012)

Ministry of Defense of Ukraine

IT Department
Department of Communications
Department of Cryptology and Information Security

THE NATIONAL CYBERSECURITY SUSTEM

The National Cybersecurity system is a set of interrelated subjects cybersecurity, which cooperate to identify, avoid and prevent cyber threats, addressing the conditions of their occurrence and minimize the negative consequences of their implementation.



NATIONAL CYBERSECURITY SYSTEM

Ensuring cybersecurity actors

Cybersecurity entities providing constant readiness

Objects of cyberprotection

Management subsystem, support for strategic decisions and coordinate the activity of cybersecurity.

The subsystem monitoring and rapid response to cyberthreats

Subsystem cyberprotection of objects of critical information infrastructure of the State

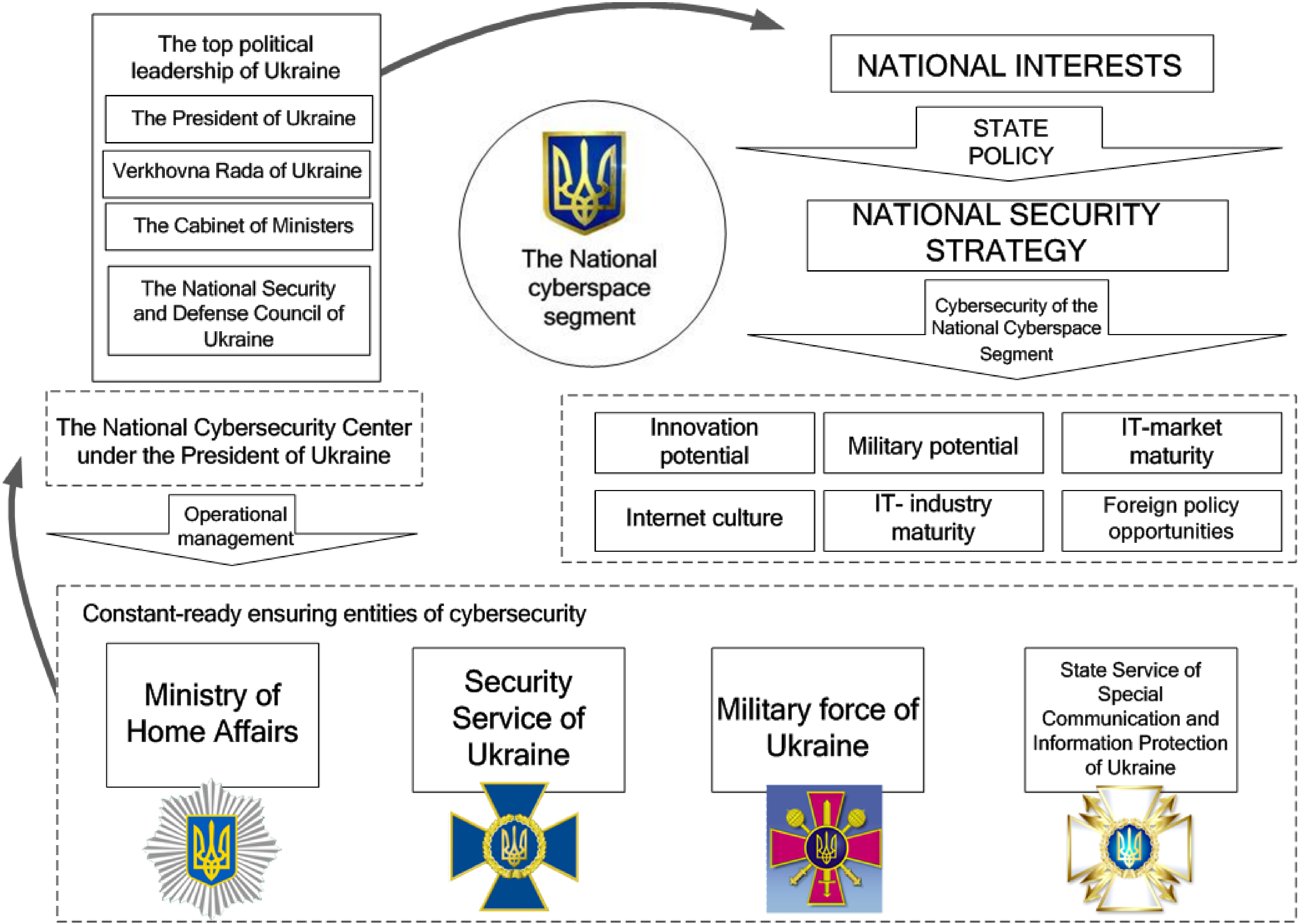
THE NATIONAL CYBERSECURITY SYSTEM

Ensuring cybersecurity actors – public authorities, local self-government armed forces and other military units, law enforcement and other government agencies as well as enterprises, institutions and organizations regardless of ownership that carry out activities related to the provision national segment of cyberspace security, including cyber provision within the provision of information and / or telecommunications services;

Cybersecurity entities providing constant readiness - state agencies or units that are part of the national system of cybersecurity, capabilities which are specifically allocated to stay in constant readiness to respond to cyber threats and resolve the tasks of ensuring cybersecurity.

The objects of cyberprotection are objects critical information infrastructure and other information and telecommunication systems, in which process the state information resources or information, protection of which is set by law.

THE NATIONAL CYBERSECURITY SYSTEM



The top political leadership of Ukraine

The President of Ukraine

Verkhovna Rada of Ukraine

The Cabinet of Ministers

The National Security and Defense Council of Ukraine

The National cyberspace segment

NATIONAL INTERESTS

STATE POLICY

NATIONAL SECURITY STRATEGY

Cybersecurity of the National Cyberspace Segment

Innovation potential

Military potential

IT-market maturity

Internet culture

IT- industry maturity

Foreign policy opportunities

The National Cybersecurity Center under the President of Ukraine

Operational management

Constant-ready ensuring entities of cybersecurity

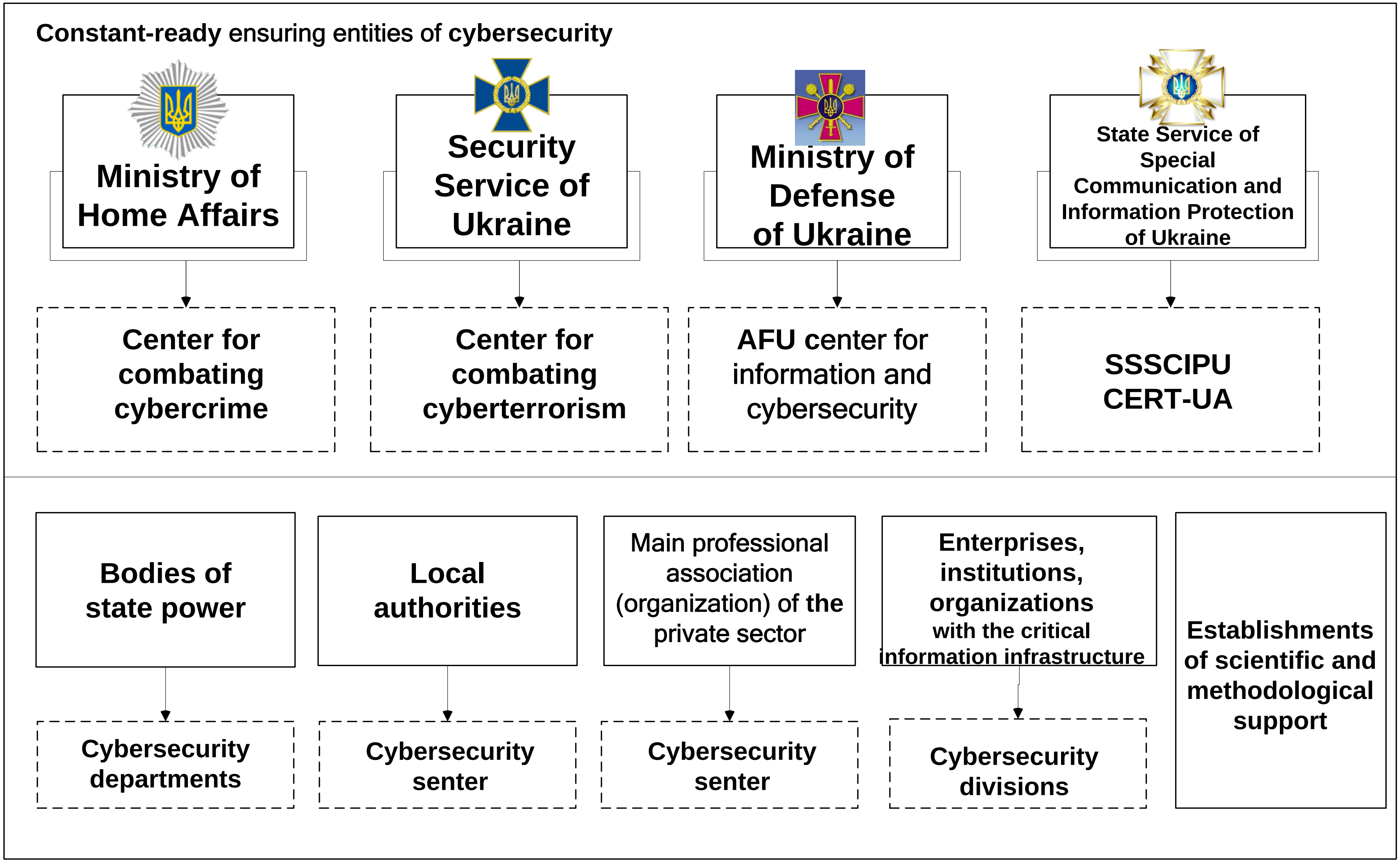
Ministry of Home Affairs

Security Service of Ukraine

Military force of Ukraine

State Service of Special Communication and Information Protection of Ukraine

THE NATIONAL SYSTEMS OF CYBERSECURITY



Constant-ready ensuring entities of cybersecurity

Ministry of Home Affairs

Center for combating cybercrime

Security Service of Ukraine

Center for combating cyberterrorism

Ministry of Defense of Ukraine

AFU center for information and cybersecurity

State Service of Special Communication and Information Protection of Ukraine

SSSCIPU CERT-UA

Bodies of state power

Cybersecurity departments

Local authorities

Cybersecurity senter

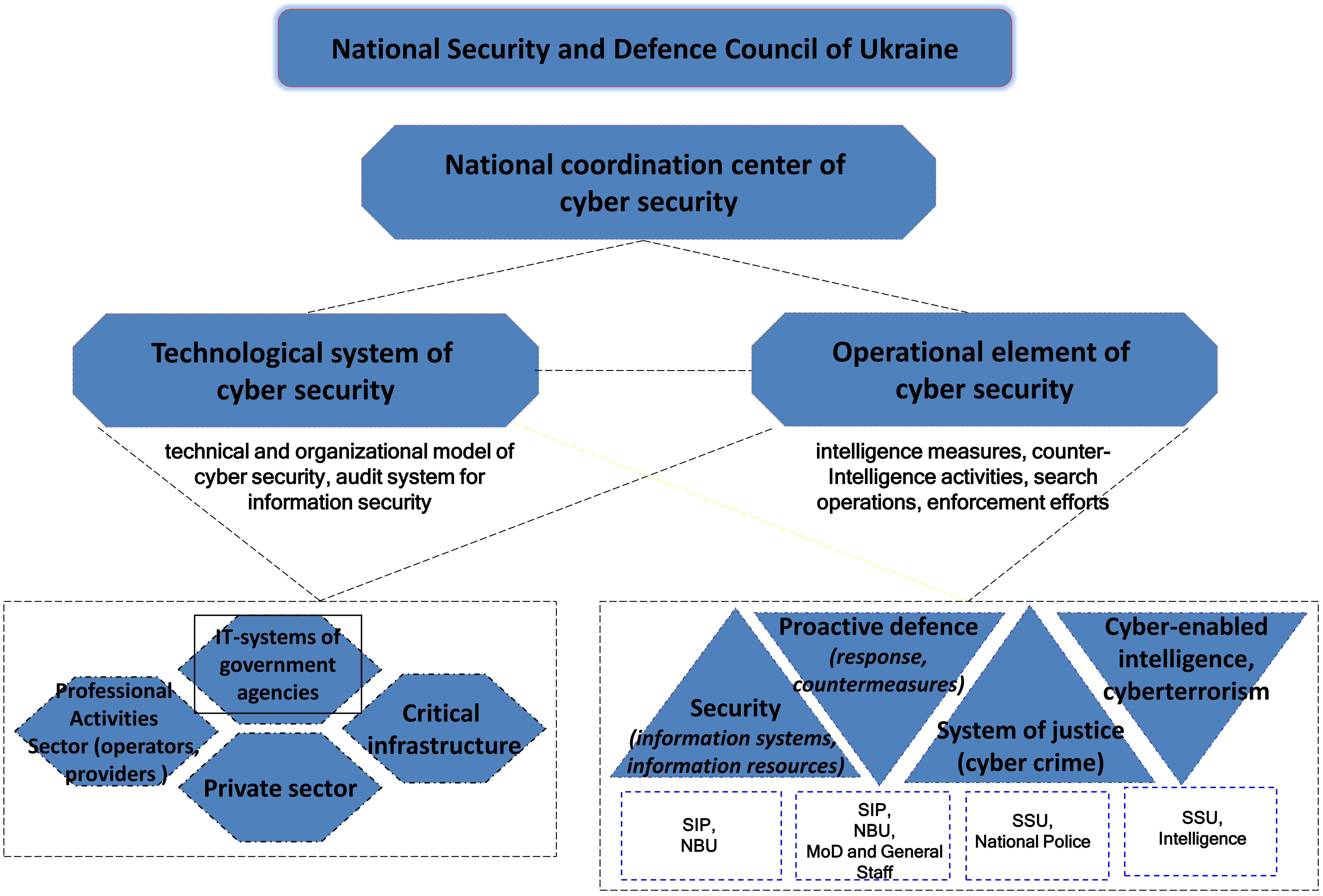
Main professional association (organization) of the private sector

Cybersecurity senter

Enterprises, institutions, organizations with the critical information infrastructure

Cybersecurity divisions

Establishments of scientific and methodological support



National Security and Defence Council of Ukraine

National coordination center of cyber security

Technological system of cyber security

Operational element of cyber security

technical and organizational model of cyber security, audit system for information security

intelligence measures, counter-Intelligence activities, search operations, enforcement efforts

IT-systems of government agencies

Professional Activities Sector (operators, providers)

Critical infrastructure

Private sector

Security *(information systems, information resources)*

Proactive defence *(response, countermeasures)*

System of justice (cyber crime)

Cyber-enabled intelligence, cyberterrorism

SIP, NBU

SIP, NBU, MoD and General Staff

SSU, National Police

SSU, Intelligence

OBJECTS

KEY SUBJECTS

CYBERSPACE

Cyberspace is recognised as the **first man-made environment**.

Like other natural environments it **cannot be controlled**.

Cyberspace, of which software forms an **intrinsic and indivisible element**, is ever evolving and an ever growing dependency for defence, yet is contingent upon a variety of **diverse participants—private firms, non-profit organisations, governments, individuals, processes, and cyber devices**.

It is therefore vital that intrinsic challenges to cyberspace—and software—are recognised and treated such that a trustworthy cyber ecosystem can be formed.

Ian Bryant *- Technical Director for Software Security,*
Dependability and Resilience at the Cyber Security Centre,
De Montfort University

FROM CYBERSECURITY SYSTEM TO SYBERSECURITY ECOSYSTEM

“Like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communication technologies) – that interact for multiple purposes.”

***“Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action”* U.S. Department of Homeland Security, 2011**

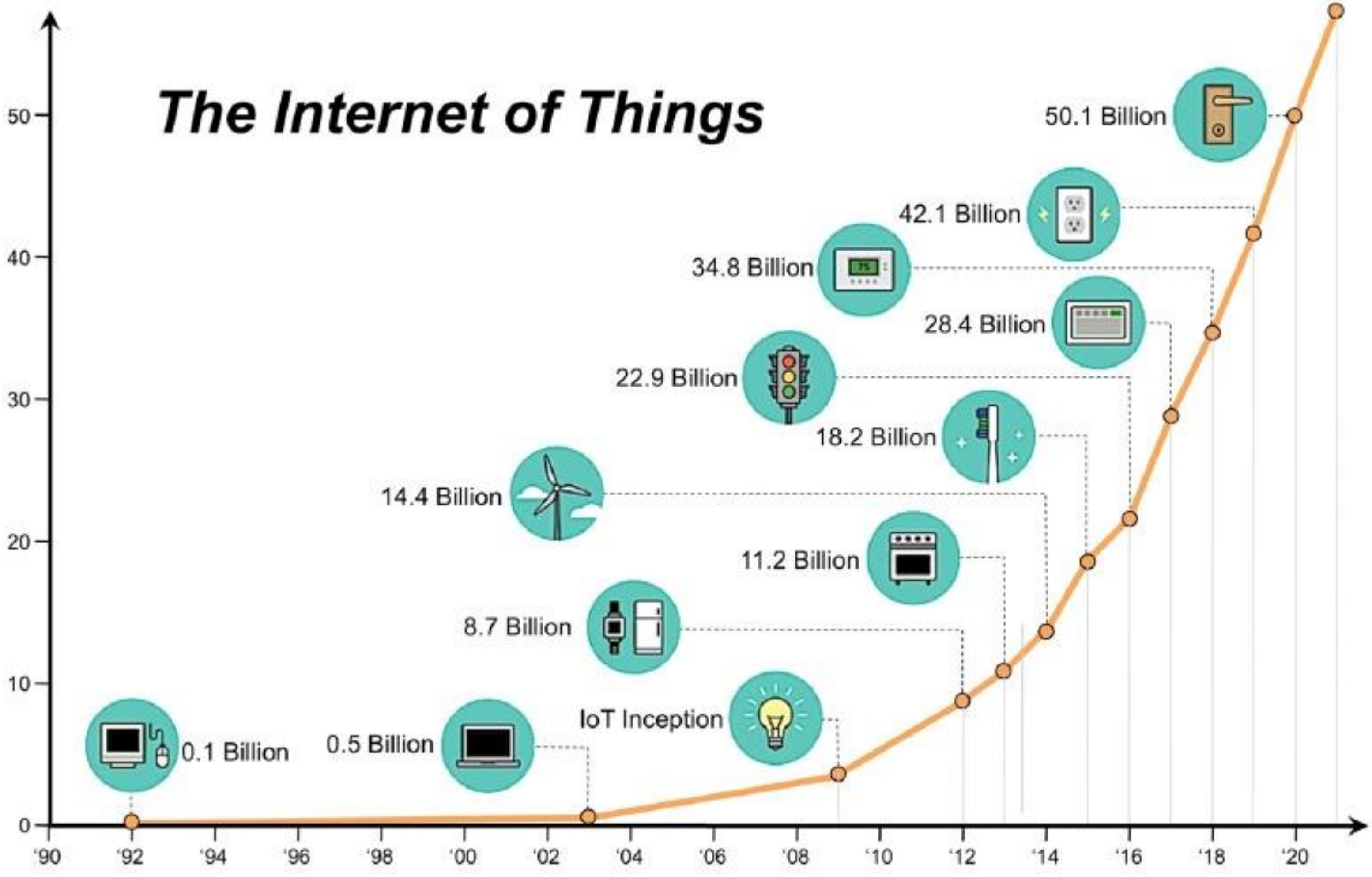
“Information security ecosystem as the network of entities that drives information security products and services, and includes information security hardware and software vendors, consultants, digital forensics experts, standardization agencies, accreditation and education facilities, academic conferences and journals, books, magazines, hackers, and their paraphernalia”

An Integrative Framework for the Study of Information Security Management Research. John D’Arcy (University of Notre Dame, USA) and Anat Hovav (Korea University, Korea)

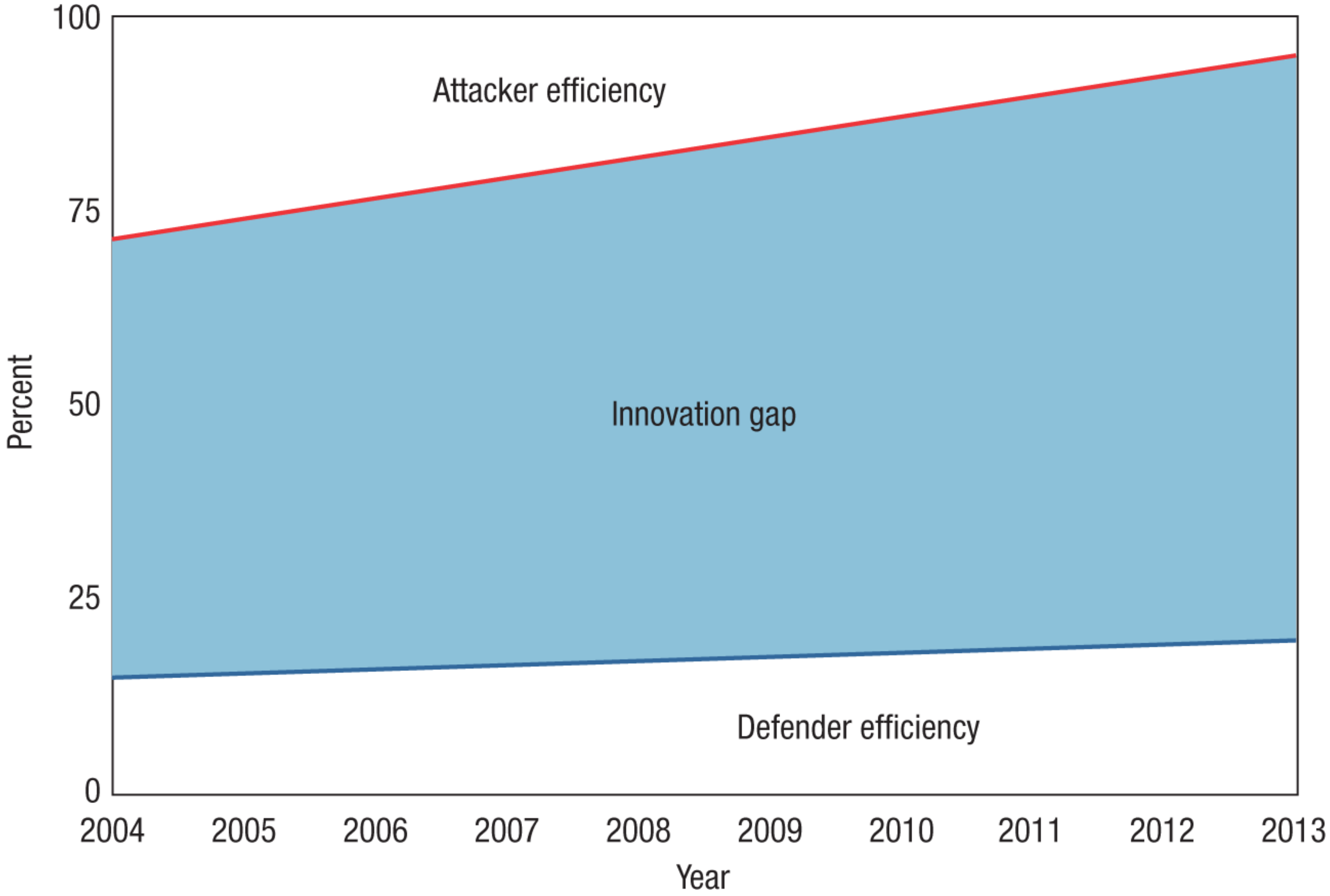
BASIC PRINCIPLE TECHNOLOGICAL ECOSYSTEM

- Inter-dependance of component
- Diversity as base of stability (harmony, unity, security and coherence)
- The technology ecosystem must evolve under the guidance of a clear and specific objective

The cyber ecosystem has been expanding much faster than the workforce can scale up to protect it, and the growth is expected to continue long into the future.



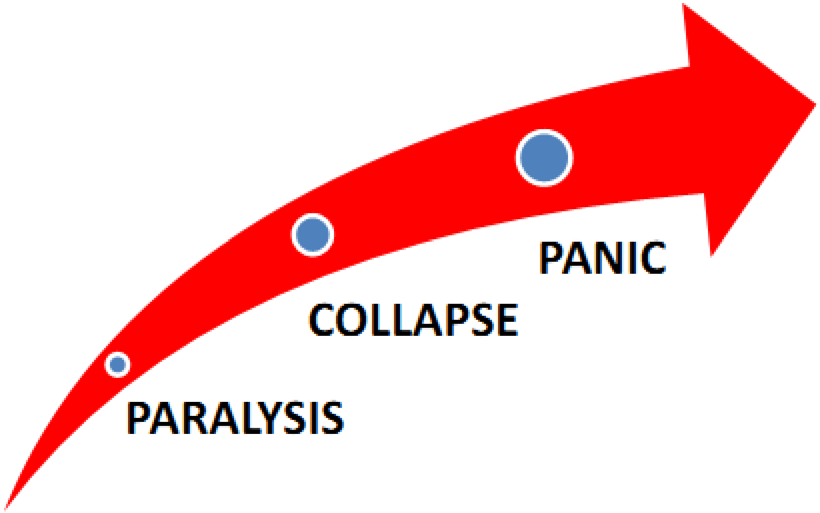
ATTACKER VERSUS DEFENDER EFFICIENCY

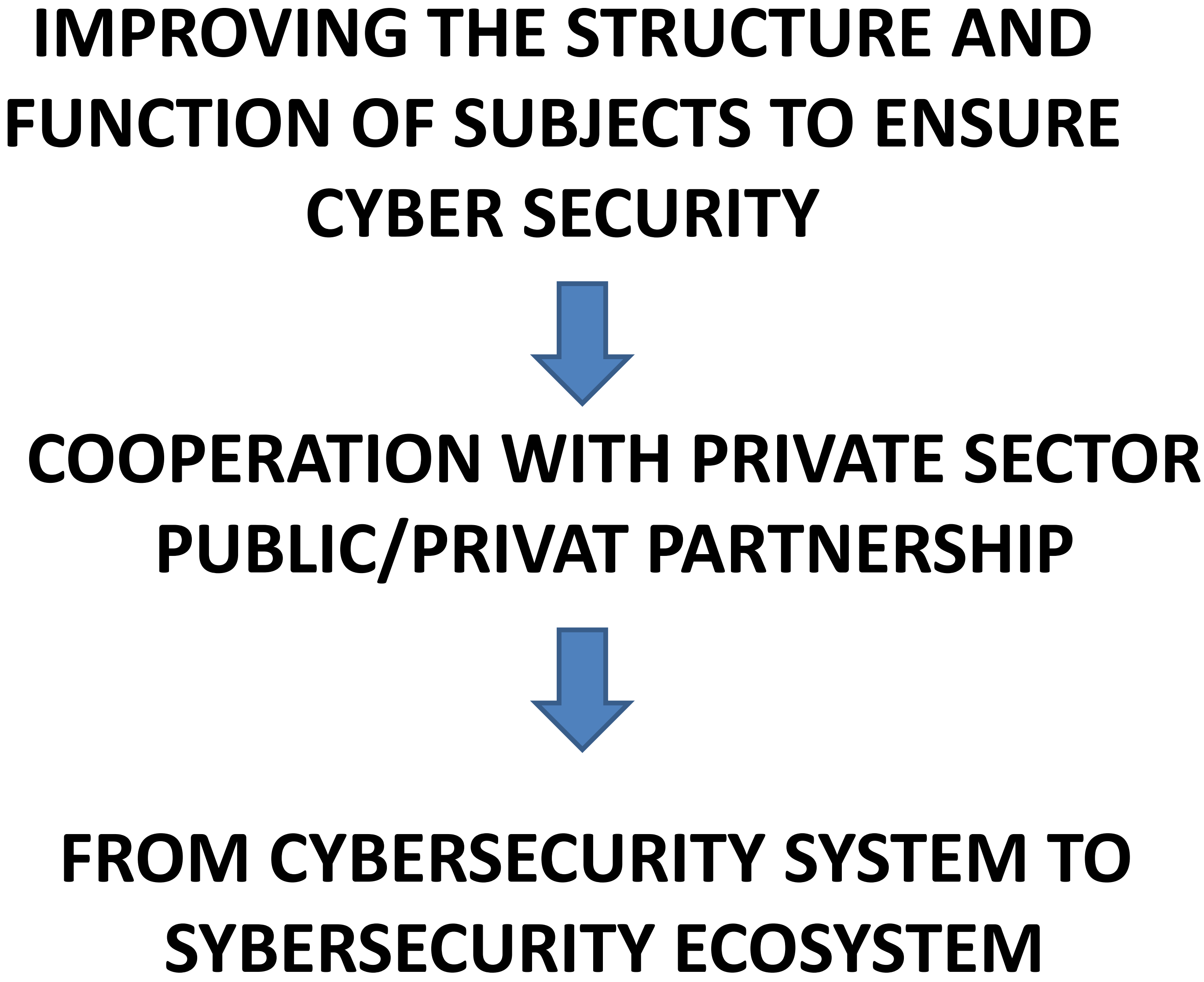


HOW CAN CYBER ATTACKS HURT NATIONAL SECURITY?

CYBER ATTACKS CAN:

- **PARALYSE** THE GOVERNMENT'S DECISION MAKING SYSTEMS
- **CRIPPLE** A NATION'S CRITICAL INFRASTRUCTURE
- CAUSE MASSIVE **PANIC** & TRIGGER INADVERTENT WARS



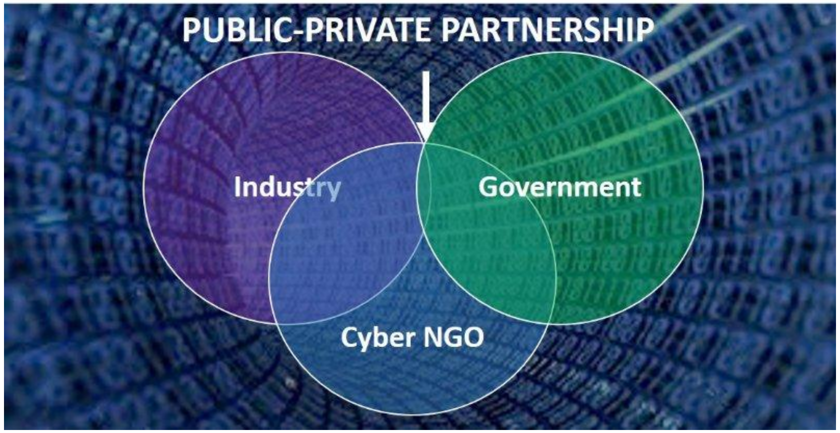


IMPROVING THE STRUCTURE AND FUNCTION OF SUBJECTS TO ENSURE CYBER SECURITY

COOPERATION WITH PRIVATE SECTOR PUBLIC/PRIVAT PARTNERSHIP

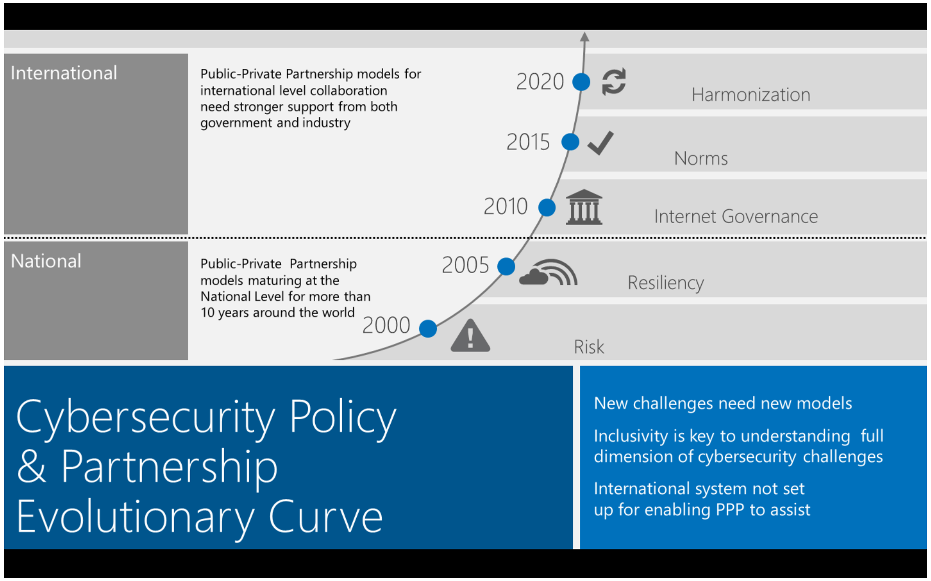
FROM CYBERSECURITY SYSTEM TO SYBERSECURITY ECOSYSTEM

PUBLIC/PRIVAT PARTNERSHIP



Government has the mission but is constrained by legal authority in cyberspace. Conversely, the private sector is not similarly constitutionally constrained, but lacks the mission.

Doug DePeppe



International

Public-Private Partnership models for international level collaboration need stronger support from both government and industry

National

Public-Private Partnership models maturing at the National Level for more than 10 years around the world

Cybersecurity Policy & Partnership Evolutionary Curve

New challenges need new models

Inclusivity is key to understanding full dimension of cybersecurity challenges

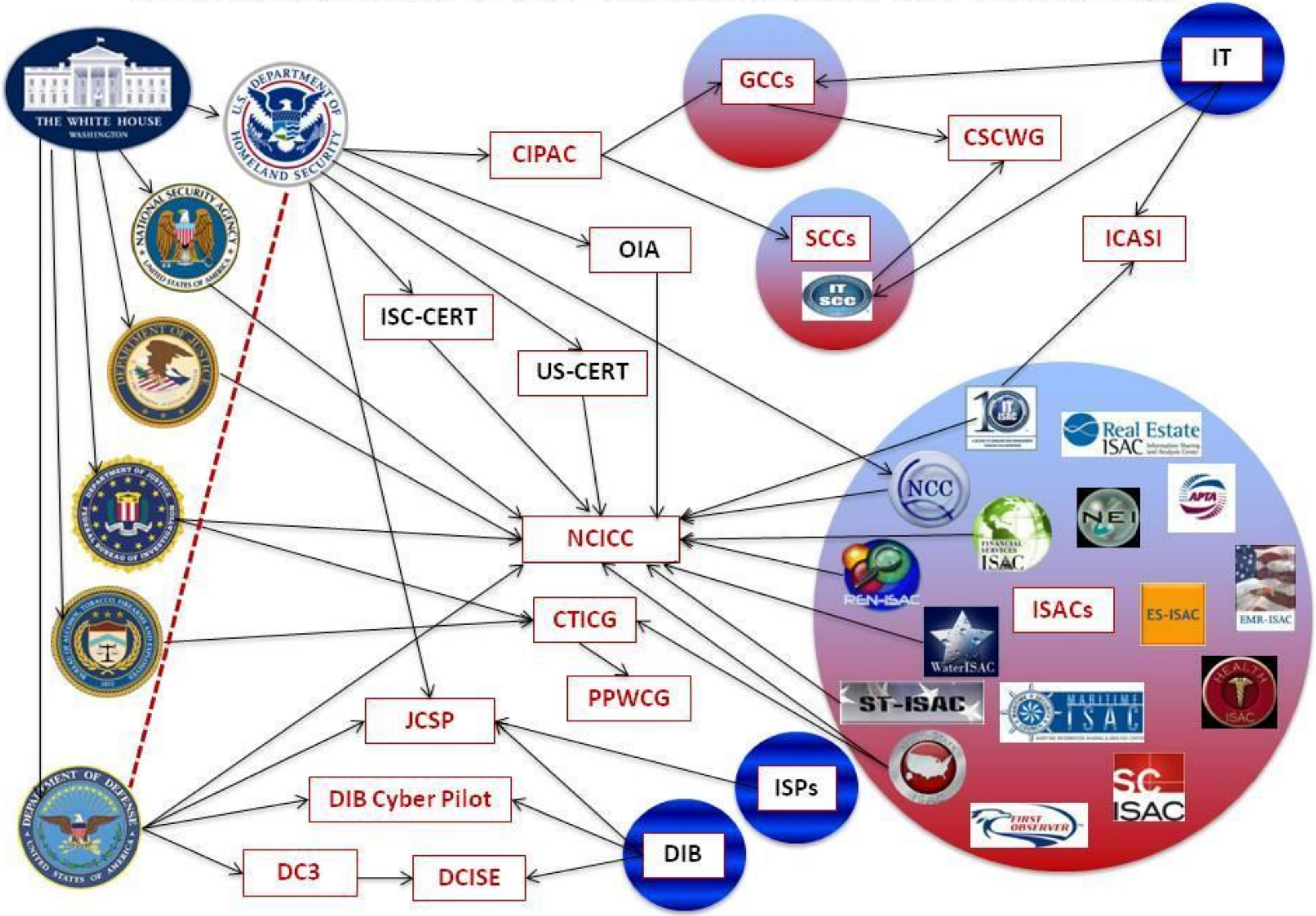
International system not set up for enabling PPP to assist

Today industry creates and operates most of the infrastructure that enables cyberspace. Industry continues to innovate and build best practices and technical cybersecurity norms including: vulnerability disclosure management, secure development, security incident response, and risk management. Therefore, these global conversations on cybersecurity would also benefit from a private sector perspective that can help governments think through the technical challenges and priorities involved in securing billions of customers using the Internet around the world.

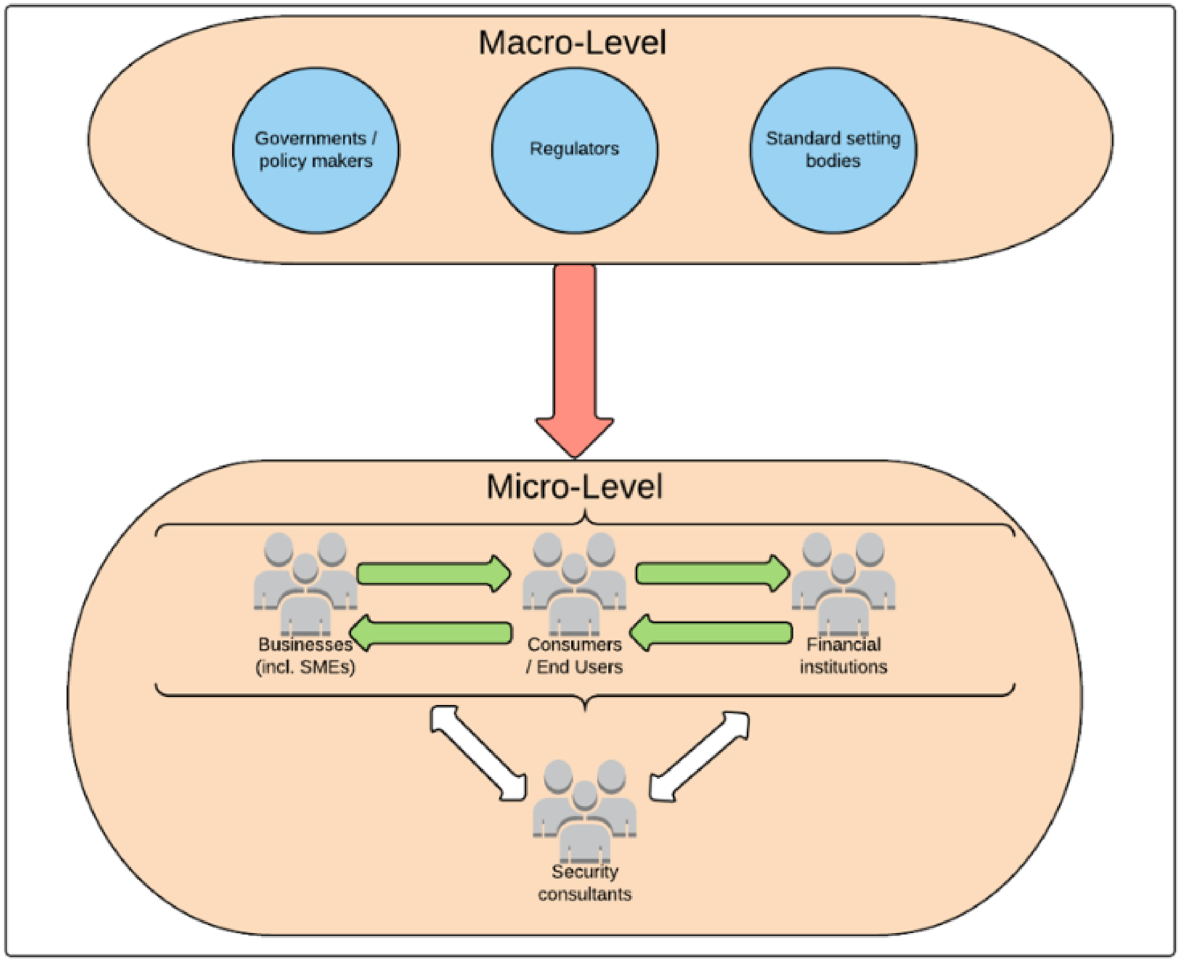
"Toward a Secure Cyber-Future: Building a Public-Private Partnership for Cybersecurity Norms.

Budapest Conference on Cyberspace 2012

Key Institutions in the Cybersecurity PPP Landscape



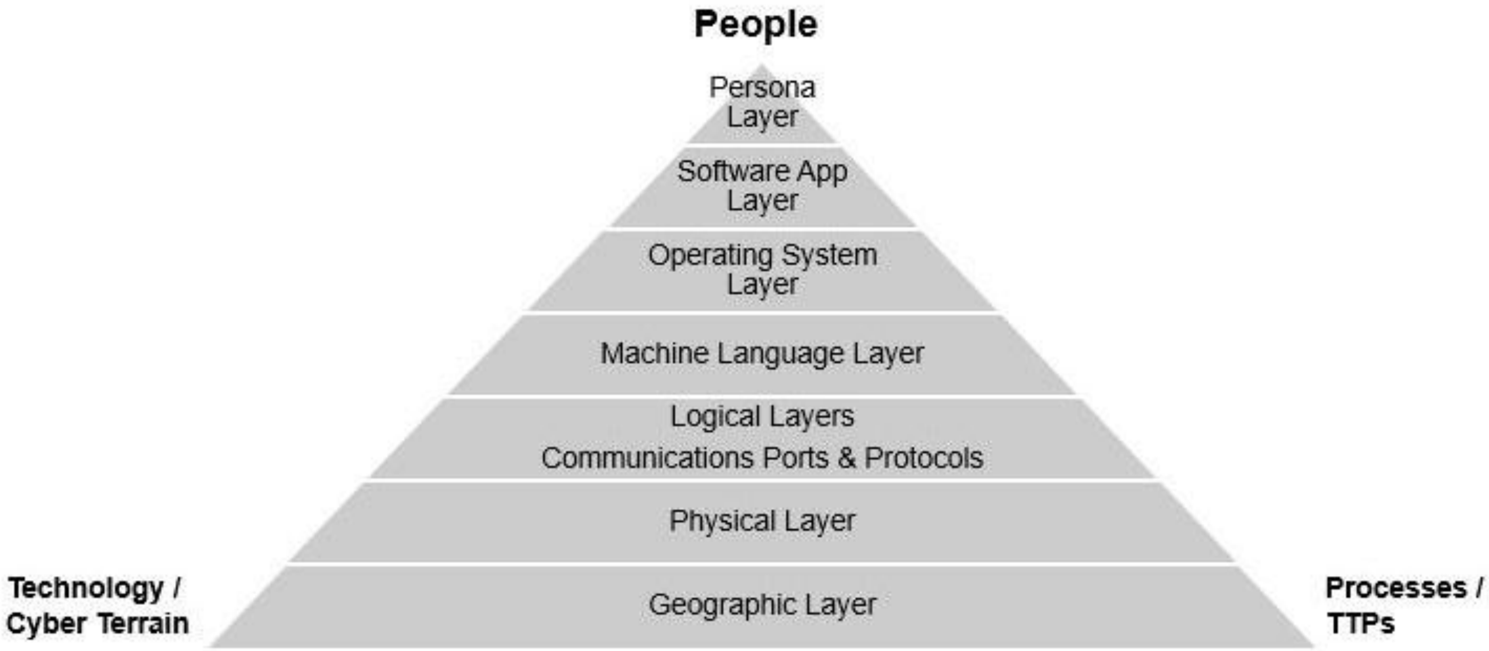
THE CYBER SECURITY ECOSYSTEM



The cyber security ecosystem

Arun Raghu. https://www.linkedin.com/pulse/cyber-security-ecosystem-collaborate-its-your-choice-arun-raghu

CYBERSECURITY ECOSYSTEM: CYBER TERRIAN LAYER MODEL by Shawn Riley



People

Persona Layer

Software App Layer

Operating System Layer

Machine Language Layer

Logical Layers
Communications Ports & Protocols

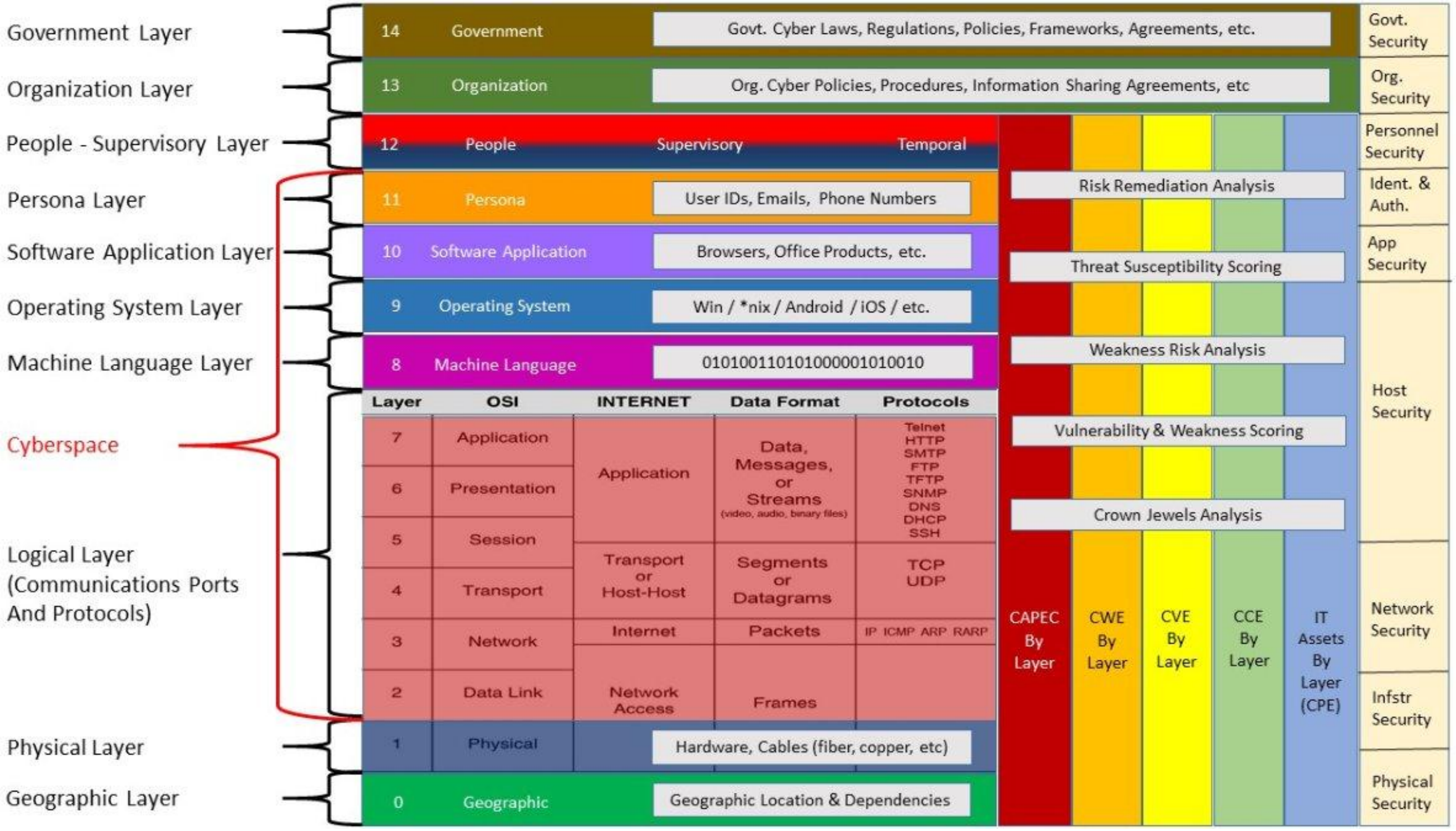
Physical Layer

Geographic Layer

Technology / Cyber Terrain

Processes / TTPs

CYBERSECURITY ECOSYSTEM: LAYER MODEL by Shawn Riley



Government Layer

Organization Layer

People - Supervisory Layer

Persona Layer

Software Application Layer

Operating System Layer

Machine Language Layer

Cyberspace

Logical Layer (Communications Ports And Protocols)

Physical Layer

Geographic Layer

14	Government	Govt. Cyber Laws, Regulations, Policies, Frameworks, Agreements, etc.		
13	Organization	Org. Cyber Policies, Procedures, Information Sharing Agreements, etc		
12	People	Supervisory	Temporal	
11	Persona	User IDs, Emails, Phone Numbers		
10	Software Application	Browsers, Office Products, etc.		
9	Operating System	Win / *nix / Android / iOS / etc.		
8	Machine Language	01010011010100001010010		

Layer	OSI	INTERNET	Data Format	Protocols
7	Application	Application	Data, Messages, or Streams (video, audio, binary files)	Telnet HTTP SMTP FTP TFTP SNMP DNS DHCP SSH
6	Presentation			
5	Session			
4	Transport	Transport or Host-Host	Segments or Datagrams	TCP UDP
3	Network	Internet	Packets	IP ICMP ARP RARP
2	Data Link	Network Access	Frames	
1	Physical	Hardware, Cables (fiber, copper, etc)		
0	Geographic	Geographic Location & Dependencies		

Risk Remediation Analysis

Threat Susceptibility Scoring

Weakness Risk Analysis

Vulnerability & Weakness Scoring

Crown Jewels Analysis

CAPEC By Layer

CWE By Layer

CVE By Layer

CCE By Layer

IT Assets By Layer (CPE)

Govt. Security

Org. Security

Personnel Security

Ident. & Auth.

App Security

Host Security

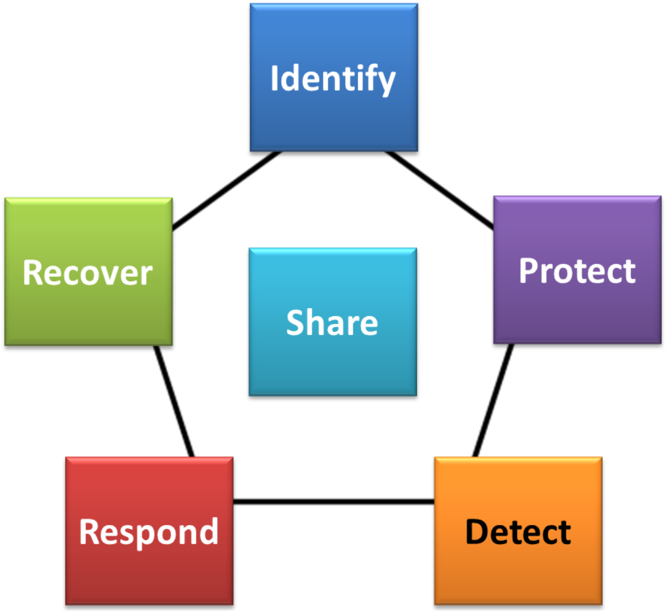
Network Security

Infstr Security

Physical Security

Global Cyber Security Ecosystem
ETSI TR 103 306 V0.5.1 (2015-02)

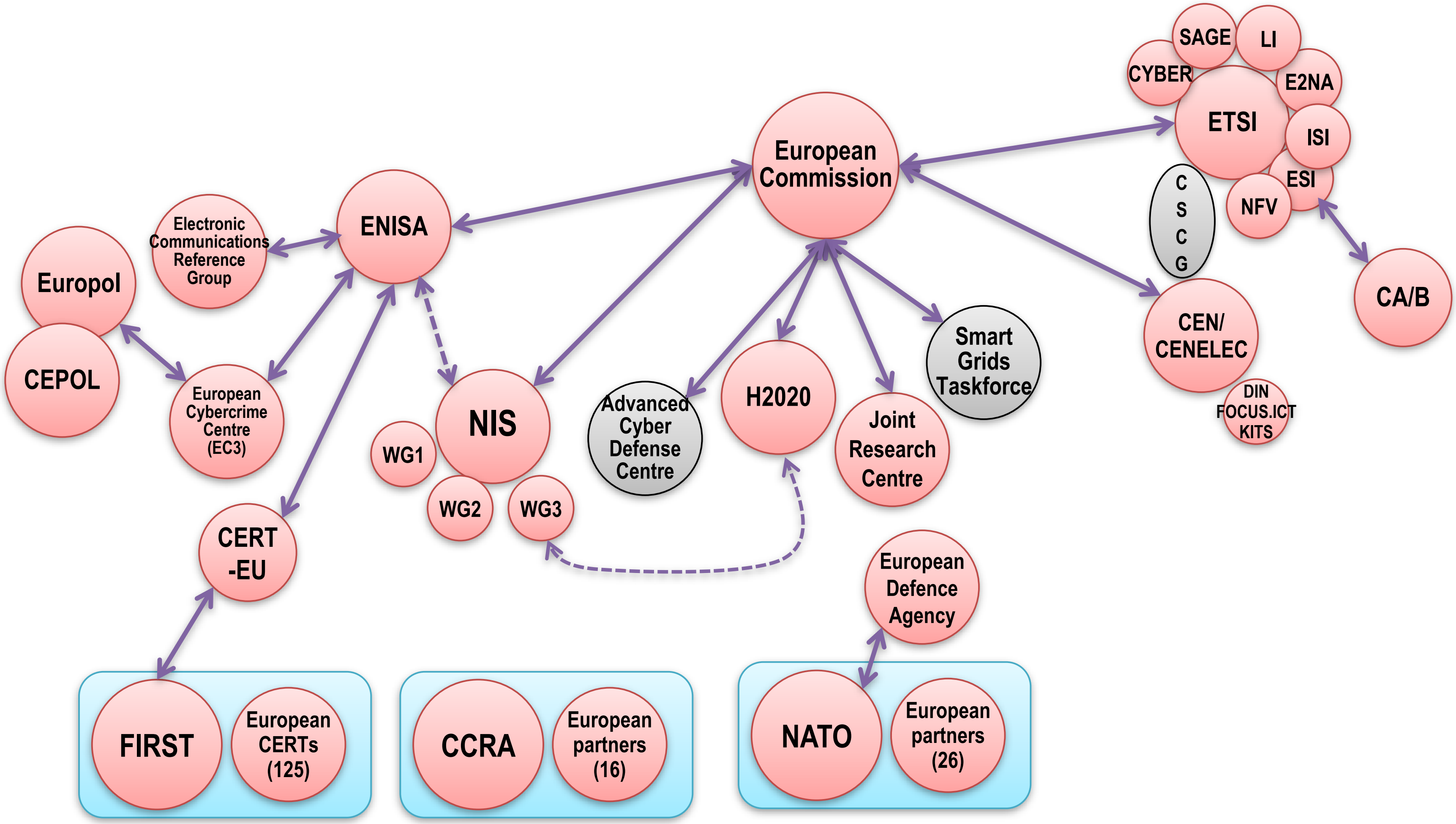
Cyber security is inherently diverse, dynamic, and spread across a complex array of bodies and activities worldwide, and constitutes a specialised ecosystem.



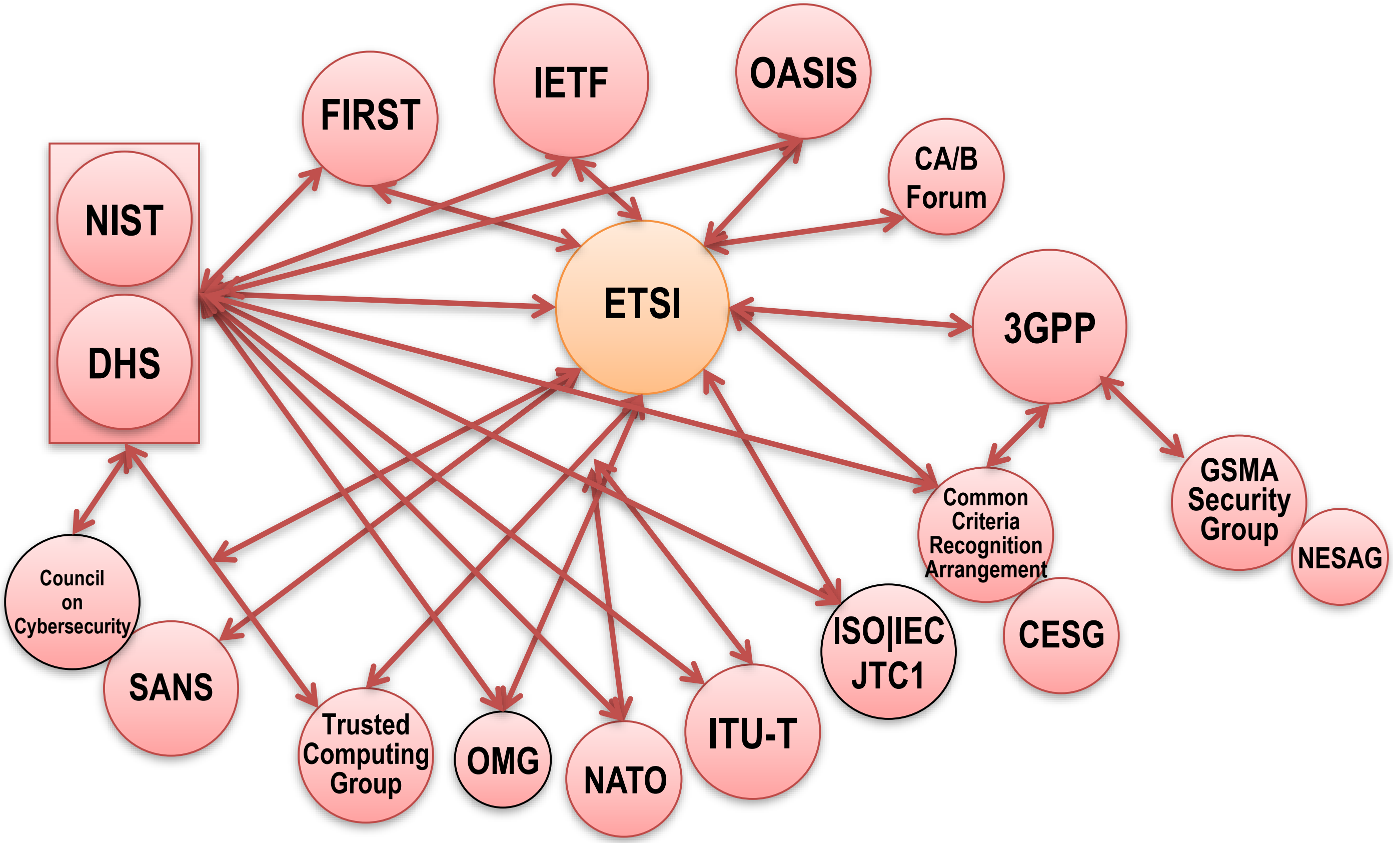
cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace

cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.

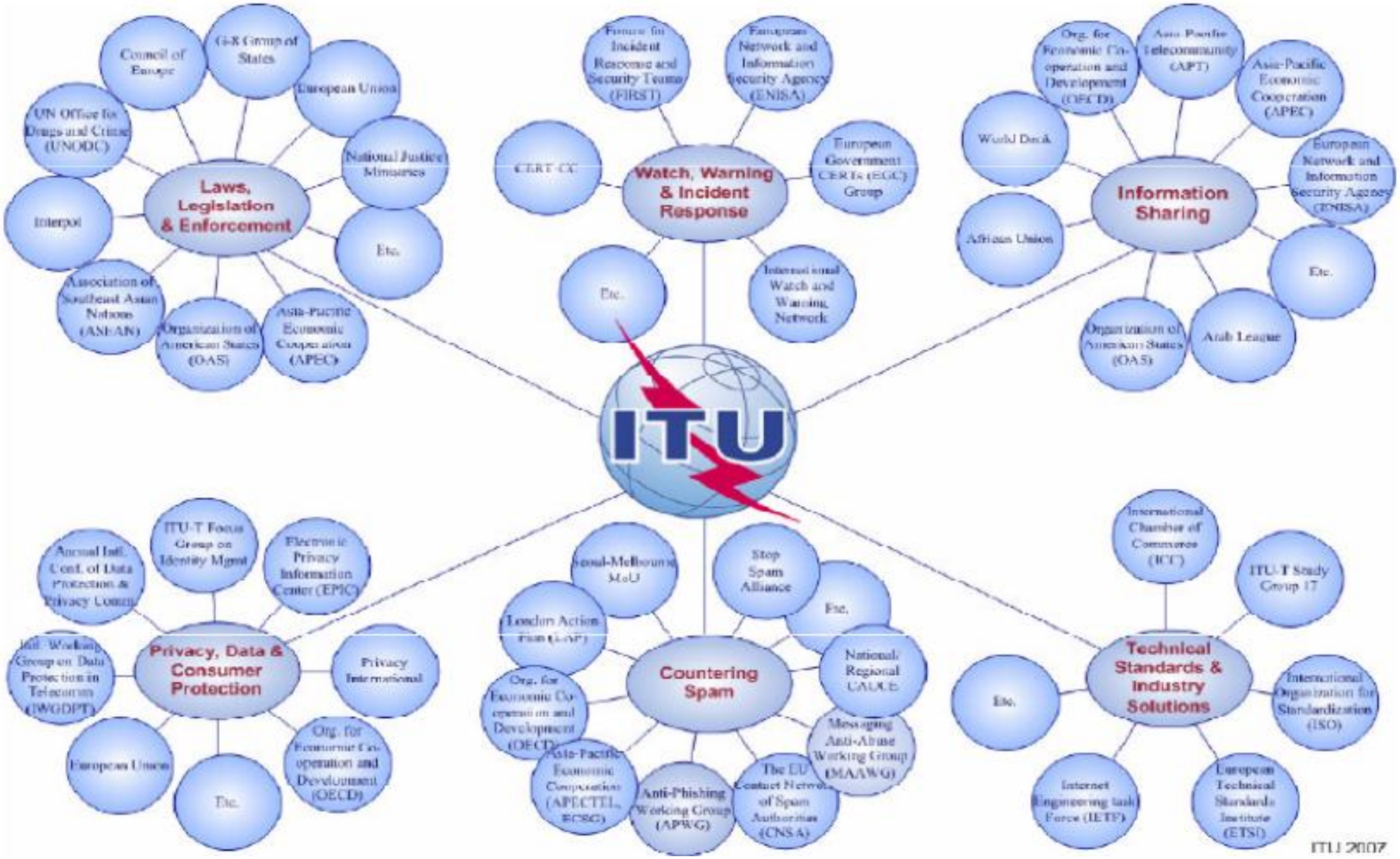
EUROPEAN CYBER SECURITY TECHNICAL ECOSYSTEM



EVOLVING GLOBAL CYBER SECURITY ECOSYSTEM



International Stakeholders for the Cybersecurity Ecosystem


Laws, Legislation & Enforcement
Council of Europe
G-8 Group of States
European Union
UN Office for Drugs and Crime (UNODC)
National Justice Ministries
Interpol
Etc.
Association of Southeast Asian Nations (ASEAN)
Organization of American States (OAS)
Asia-Pacific Economic Cooperation (APEC)
Watch, Warning & Incident Response
Forum for Incident Response and Security Teams (FIRST)
European Network and Information Security Agency (ENISA)
CERT-CC
European Government CERTs (EGC) Group
Etc.
International Watch and Warning Network
Information Sharing
Org. for Economic Co-operation and Development (OECD)
Asia-Pacific Telecommunity (APT)
Asia-Pacific Economic Cooperation (APEC)
World Bank
European Network and Information Security Agency (ENISA)
African Union
Etc.
Organization of American States (OAS)
Arab League
ITU
Privacy, Data & Consumer Protection
Annual Intl. Conf. of Data Protection & Privacy Comm.
ITU-T Focus Group on Identity Mgmt
Electronic Privacy Information Center (EPIC)
Intl. Working Group on Data Protection in Telecomm (IWGDPT)
Privacy International
European Union
Etc.
Org. for Economic Co-operation and Development (OECD)
Countering Spam
Seoul-Melbourne MoU
Stop Spam Alliance
Etc.
London Action Plan (LAP)
National Regional CAUCE
Org. for Economic Co-operation and Development (OECD)
Messaging Anti-Abuse Working Group (MAAWG)
Asia-Pacific Economic Cooperation (APECTEL, ECSG)
Anti-Phishing Working Group (APWG)
The EU Contact Network of Spam Authorities (CNSA)
Technical Standards & Industry Solutions
International Chamber of Commerce (ICC)
ITU-T Study Group 17
Etc.
International Organization for Standardization (ISO)
Internet Engineering task Force (IETF)
European Technical Standards Institute (ETSI)

ITU 2007

CYBERSECURITY ECOSYSTEM: WHAT WE NEED DO?

Legal Framework:

- Does the country have an adequate legal model for security and privacy?
- Does the current legislative eco-system understand new age complexities?
- Whether special legislation is enacted to deal with specific challenges imposed by for Information Technology?

Government Initiatives:

- Is the government proactive enough in policy enablement?
- Does it invest enough to address increasing challenges?
- How does it partner and collaborate with industry, academia and other stakeholders?

Special Projects:

- What projects have been under taken at the national level that affects cyber space and privacy?
- How will these projects benefit the cause?

Industry Initiatives:

- How are the industries participating and collaborating in the eco-system?
- Is there any specially purpose mechanism established that provides a suitable platform to the industry?

Law enforcement:

- Is law enforcement in the country effective enough to handle the new age crimes ?
- What initiatives have been taken for improving law enforcement?

Thank you for attention!

Feel free to ask questions