CYBERSECURITY ECOSYSTEM

Prof. Oleksandr POTII

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 CYBERSPACE TO CYBER ECOSYSTEM

- Cyberspace is now acknowledged to be the first **man-made environment**
- cyberspace does not erase spatial boundaries—rather the transnational dimension opened up by cyberspace allows for anonymity
- cyberspace challenge the defining assumptions that underpin conceptions about competent authority, jurisdictions, conflict, criminality, cash, and the use of force.
- Protecting the infrastructure becomes all the more essential against the impacts of disruptions and cyber attacks because the forces at work in cyberspace may more readily be asymmetric, that is, unconventional and disproportionate
- Trustworthy cyberspace is vital to the prospects of enhancing a government's reputation for trusted and reliable hubs and networks, but the evolution of cyberspace is uncertain.
- Developments of cyber, bio, and nanotechnology are morphing into one another, and the boundaries between users and developers is blurring.

DEPENDENCE FROM ICT AND SOFTWARE

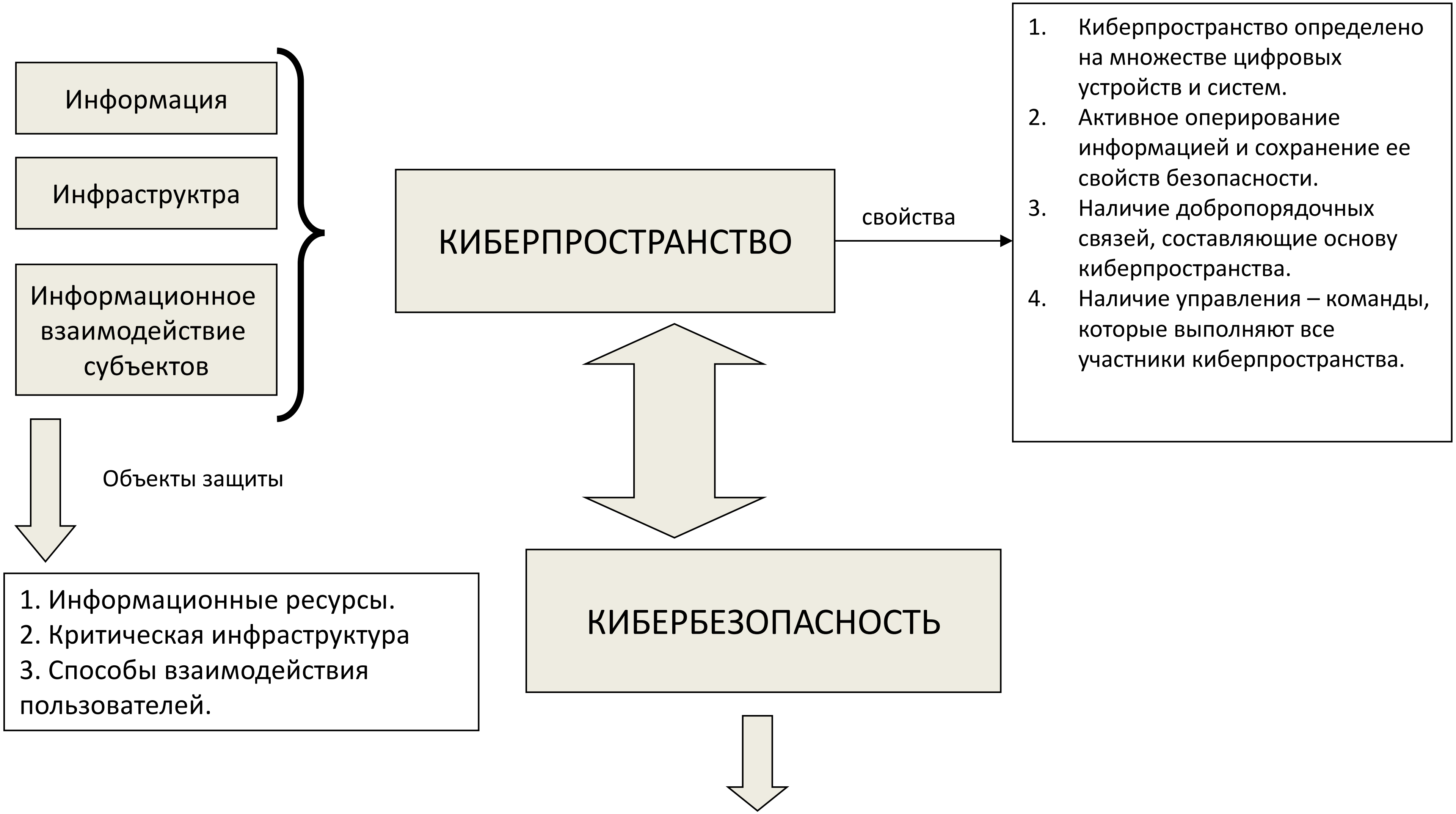
- The move to distributed application platforms and services, where the boundaries of organisation and/or national jurisdiction are increasingly blurred, and the options for either proactive controls and/or reactive measures are similarly constrained.
- Increasing reliance on mobile devices, such as smartphones and tablets, which typically rely on lightweight operating systems with less inherent controls than operating systems of previous generation desktop devices.
- A move in business to consumerization and Bring Your Own Device, where the boundary of ownership is blurred between the organization and the individuals who work for the organization.
- Commoditization in previously closed architectures, such as industrial control systems where, for instance, a step change is being encountered of previously bespoke sensor devices with wireline connections to proprietary control systems are being replaced by configurable, off-the-shelf sensors using wireless connections to generic ICT systems that have onward connections to the global internet.
- The pressure for ICT consolidation for energy efficiency for green reasons (the low carbon imperative) leading to extensive use of software virtualization to separate previously physically distinct services.

CHANGING WAYS DEVELOPED AND DEPLOYED OF SYSTEMS

- The adoption of open source models for sourcing software, fundamentally disrupting views of single organisational control.
- The growth of multicore processor technologies, which can subvert the risk modelling approaches used in previous generations of hardware.
- Growing questions as to whether hardware platforms used for software can be trusted to execute as expected, with evidence of counterfeit hardware being found in multiple market segments.
- A blurring of the boundary between software and hardware boundary, for instance with the use of software style design languages to implement application-specific integrated circuits and field-programmable gate arrays.
- The increasing use of generic, self-documenting structured data (e.g. XML) to control systems’ behaviours rather than rely on pre-defined execution paths.

SOFTWARE DEVELOPMENT

- The adoption of other approaches such as agile and rapid application development by the software industry.
- The growth in small-scale software development, typically carried out by micro-business who will not invest in formal development approaches, as exemplified by the apps movement for smartphones and tablets.
- A plethora of activity which produces artifacts that have the properties of software, as exemplified by the mass of websites which use, to a greater or lesser extent, mobile or active code (such as Java, Javascript and ActiveX). In these cases many of the users will have little, if any, awareness that they are implicitly creating software functionality by their often point-and-click activities.



1. Киберпространство определено на множестве цифровых устройств и систем.
2. Активное оперирование информацией и сохранение ее свойств безопасности.
3. Наличие добропорядочных связей, составляющие основу киберпространства.
4. Наличие управления – команды, которые выполняют все участники киберпространства.

1. Информационные ресурсы.
2. Критическая инфраструктура
3. Способы взаимодействия пользователей.

Цель – обеспечения безопасности (защита) деятельности людей, которая осуществляется с помощью информационных активов, обрабатываемых посредством критической инфраструктуры

SECURITY AND RESILIENCE

Security and resilience for cyberspace to be seen as not just a service but are the services underpinning trust and confidence in an environment that touches all others”

MacIntosh, JP, Reid J & Tyler, L*; Cyber Doctrine: Towards A Coherent Evolutionary Framework for Learning Resilience; Institute for Security & Resilience Studies*

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

FROM CYBERSECURITY SYSTEM TO SYBERSECURITY ECOSYSTEM

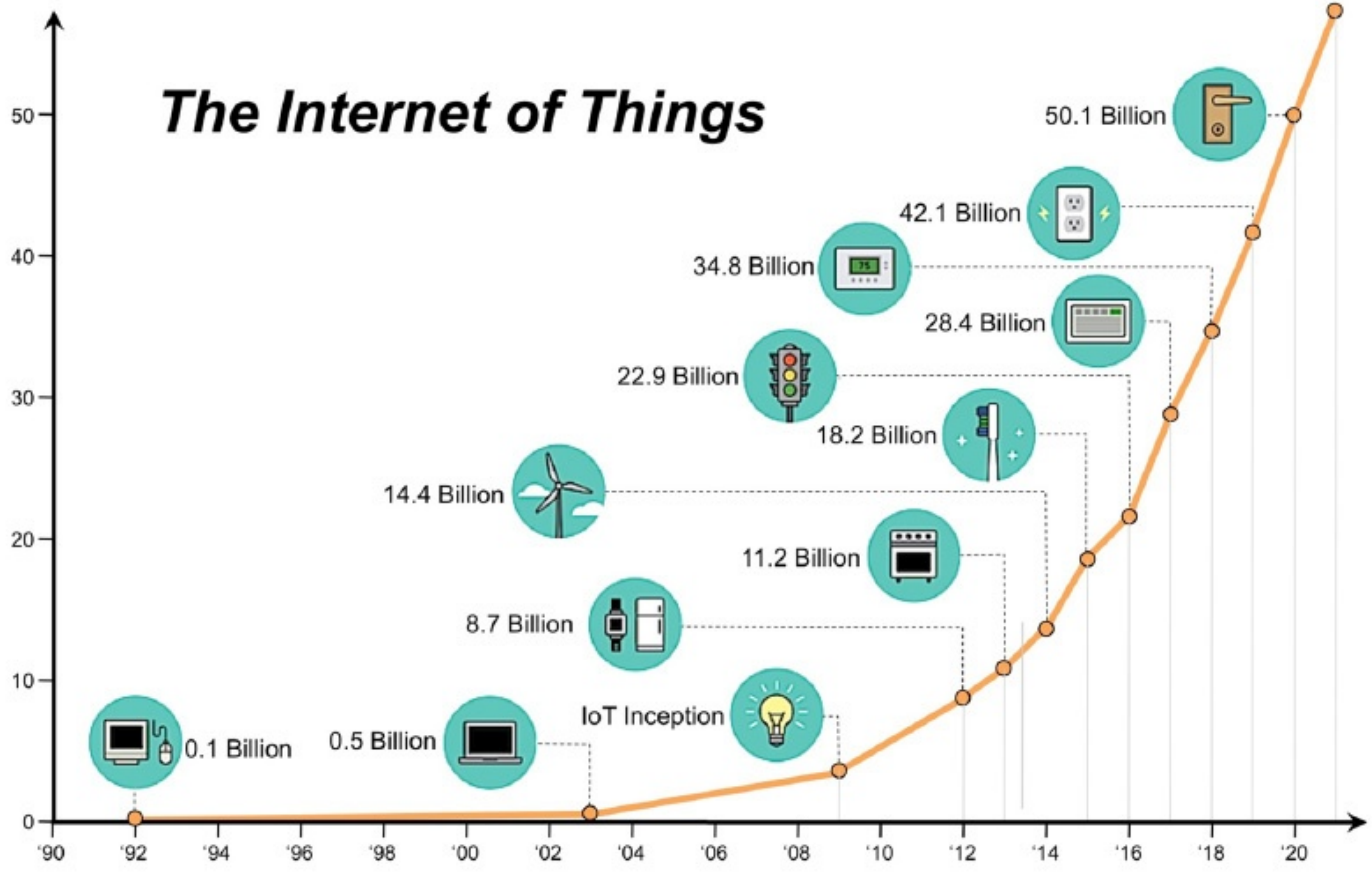
“Like natural ecosystems, the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communication technologies) – that interact for multiple purposes.”

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

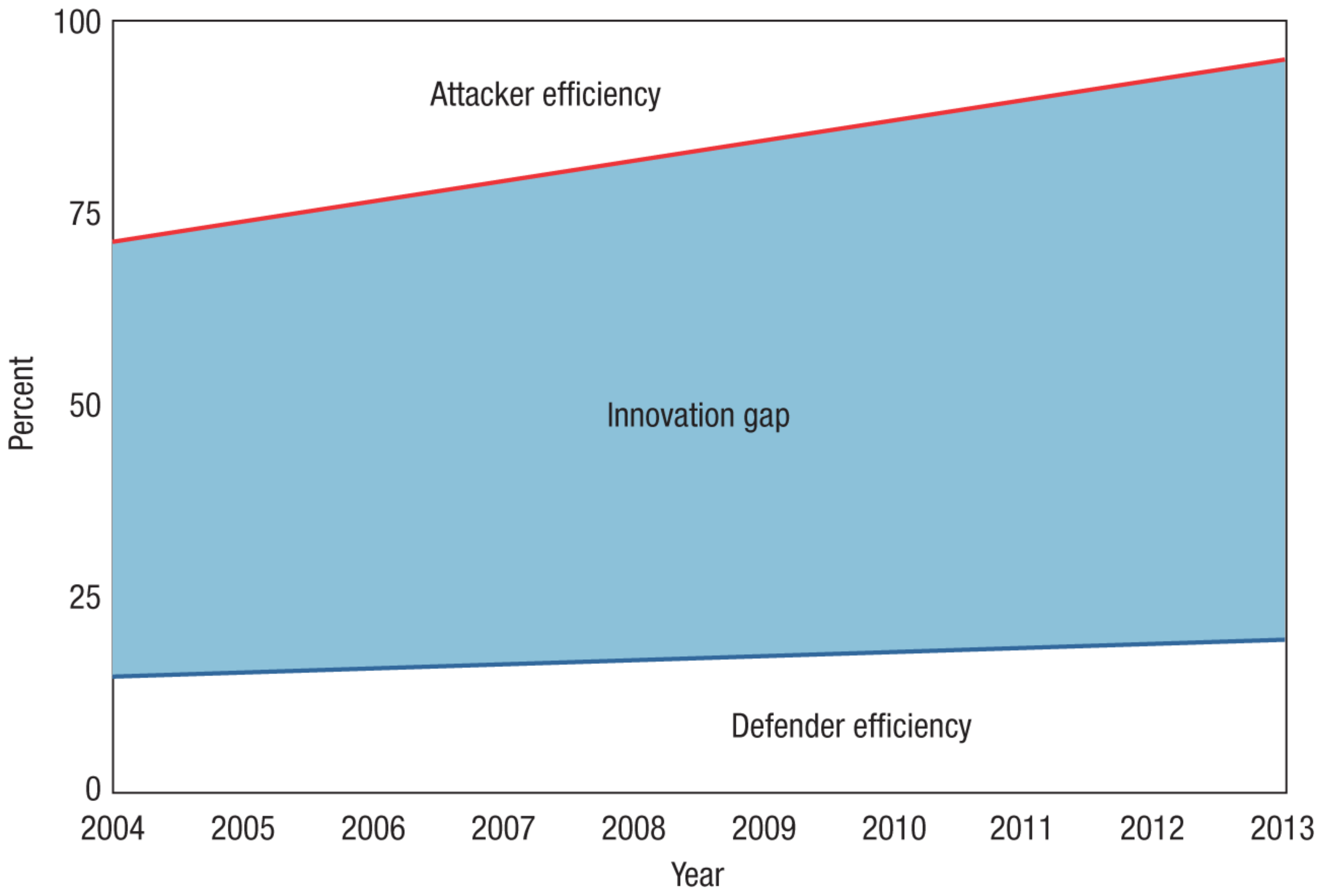
“**Information security ecosystem** as the network of entities that drives **information security** products and services, and includes **information security** hardware and software vendors, consultants, digital forensics experts, standardization agencies, accreditation and education facilities, academic 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)*

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.



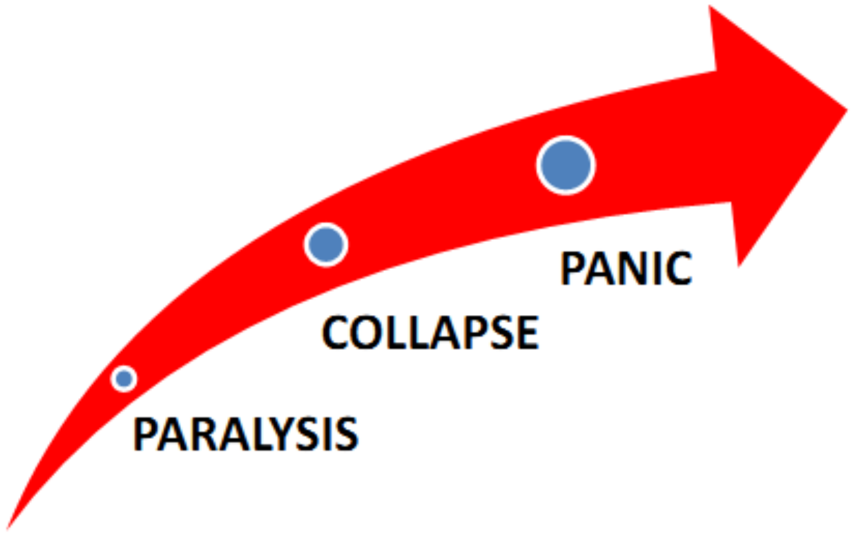
ATTACKER VERSUS DEFENDER EFFICIENCY



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



Cases of Cyber Warfare/Attack

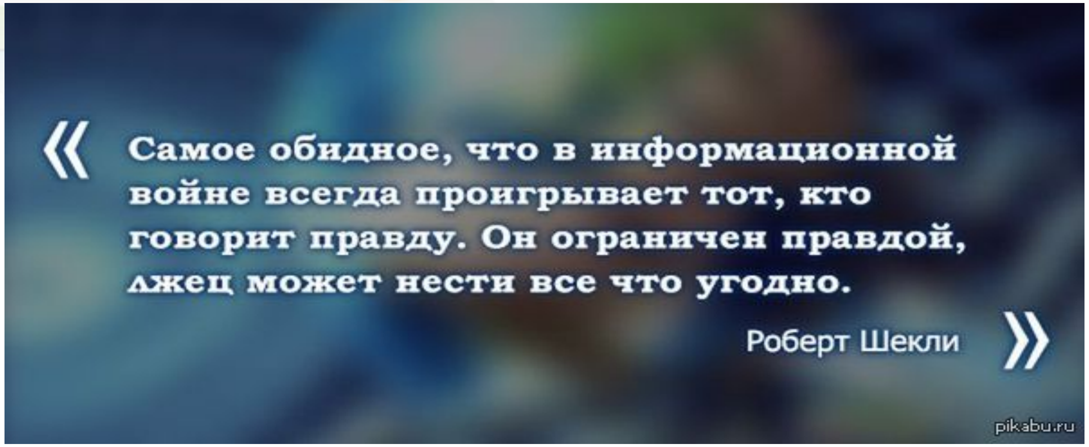
File Edit View Favorites Tools Help
Back
Address http://www.president.gov.ge/

Russia-Georgia Cyber warfare 2008

Wikileaks

STUXNET

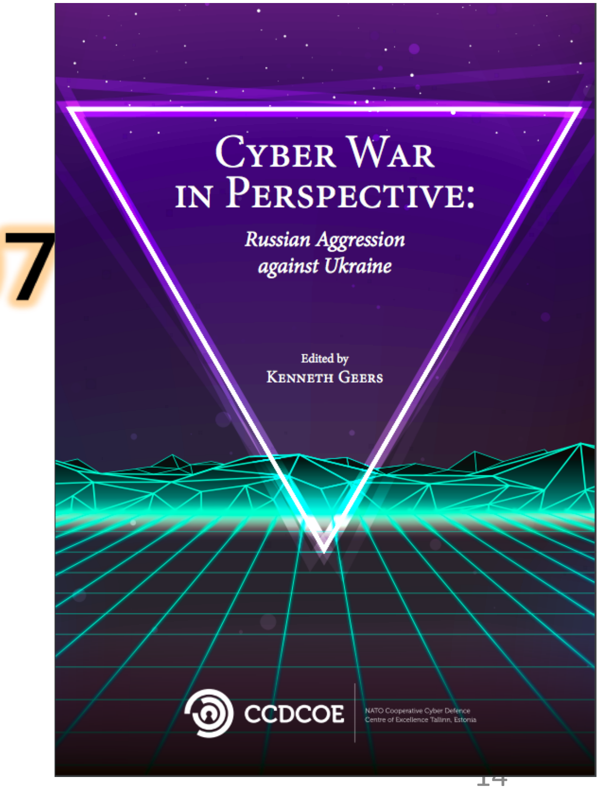
Estonia Cyber Attack 2007



« Самое обидное, что в информационной войне всегда проигрывает тот, кто говорит правду. Он ограничен правдой, лжец может нести все что угодно.

Роберт Шекли »

pikabu.ru

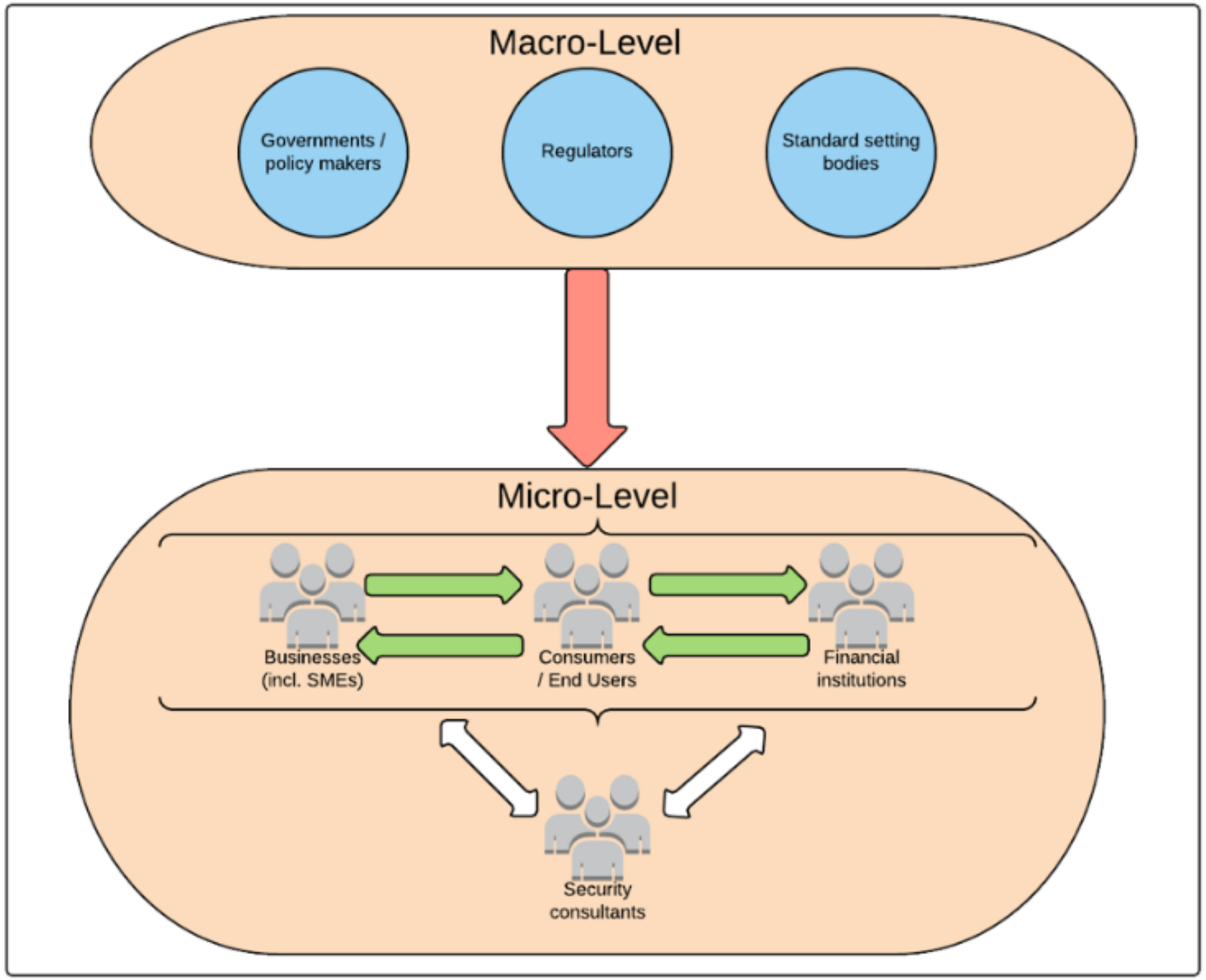


Cyber War in Perspective: Russian Aggression against Ukraine

Edited by Kenneth Geers

CCDCOE NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

THE CYBER SECURITY ECOSYSTEM



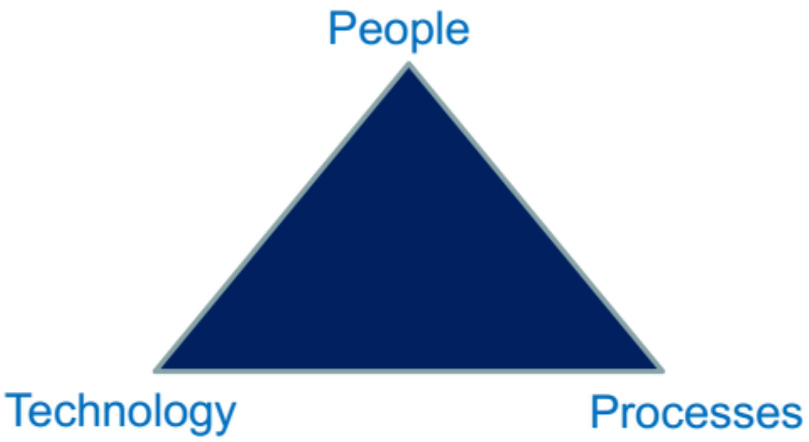
The cyber security ecosystem

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

CYBER ECOSYSTEM

- Ecosystem is defined as “a community of living organisms in conjunction with the nonliving components of their environment, interacting as a system”.
- DHS defines a cyber ecosystem as:

  “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.”



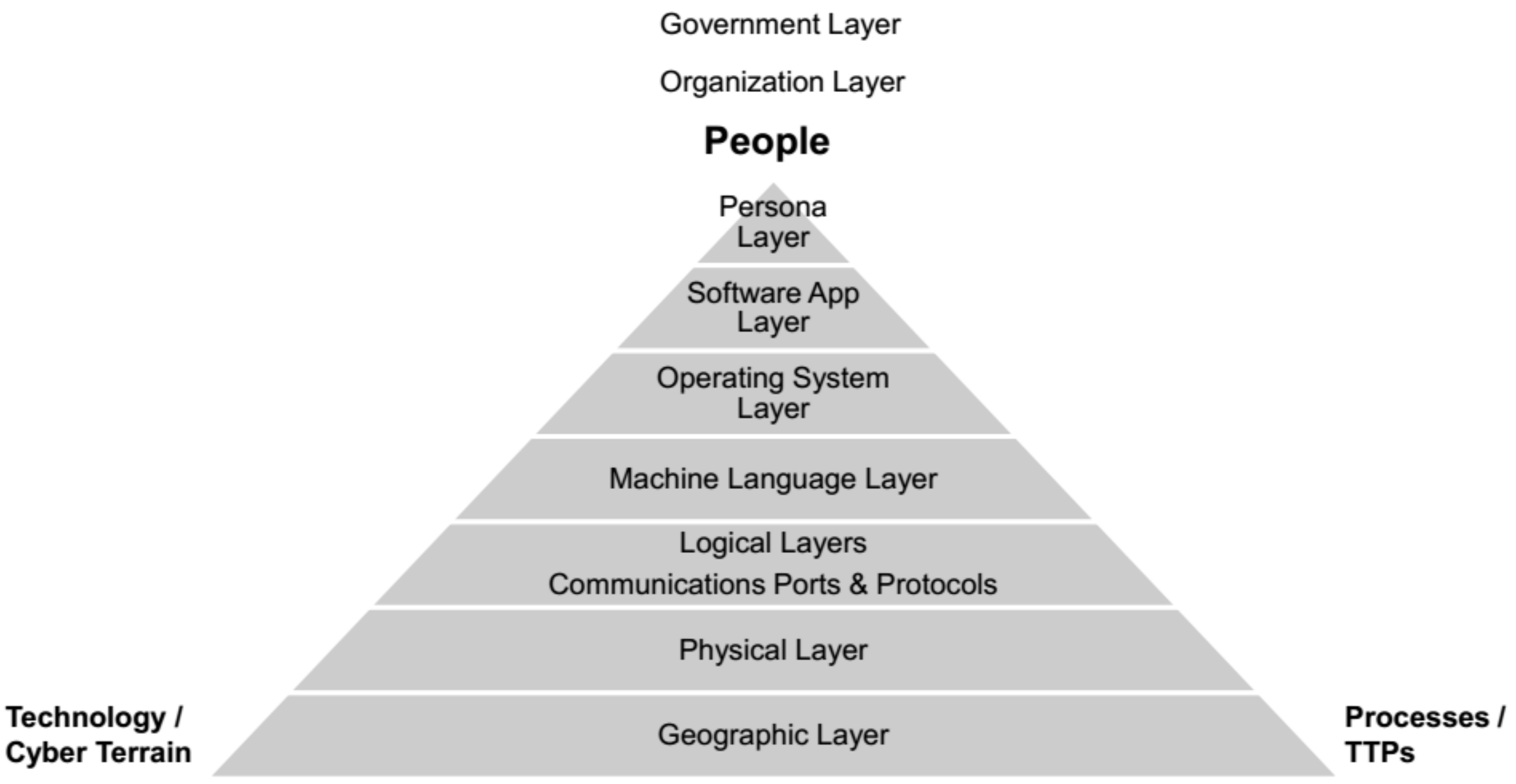
People

Technology

Processes

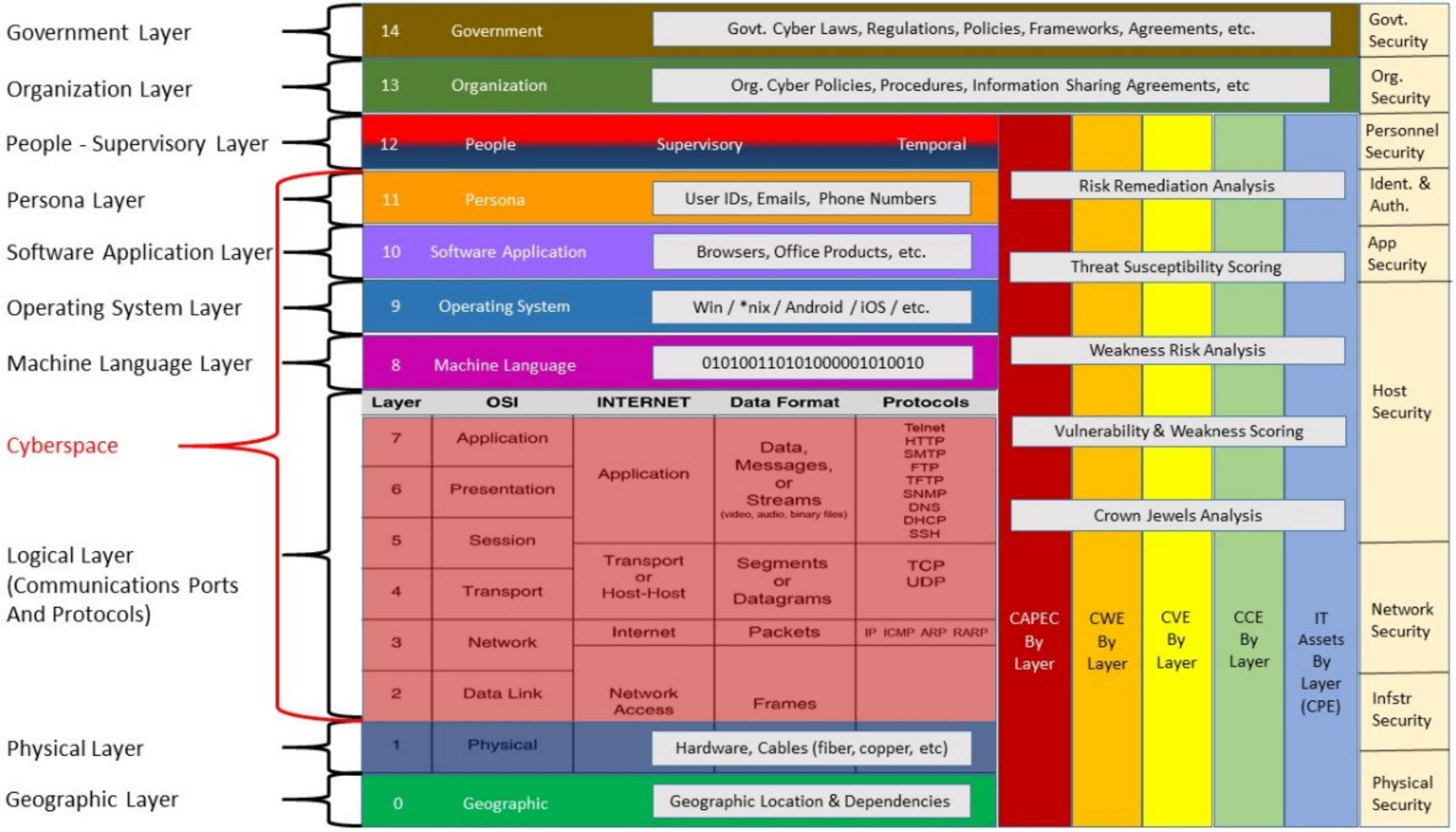
http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

CYBERSECURITY ECOSYSTEM: CYBER TERRIAN LAYER MODEL by Shawn Riley



http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

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. — Govt. Security

13 Organization — Org. Cyber Policies, Procedures, Information Sharing Agreements, etc — Org. Security

12 People — Supervisory — Temporal — Personnel Security

11 Persona — User IDs, Emails, Phone Numbers — Ident. & Auth.

10 Software Application — Browsers, Office Products, etc. — App Security

9 Operating System — Win / *nix / Android / iOS / etc.

8 Machine Language — 010100110101000001010010

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)

Host Security

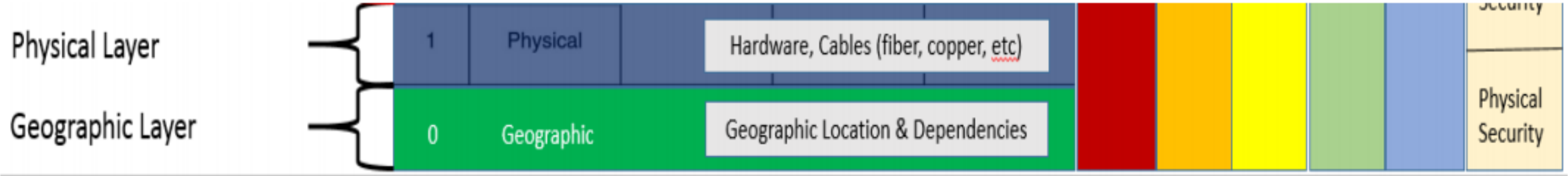
Network Security

Infstr Security

Physical Security

From Science of Security: Cyber Intelligence Analysis Shawn Riley

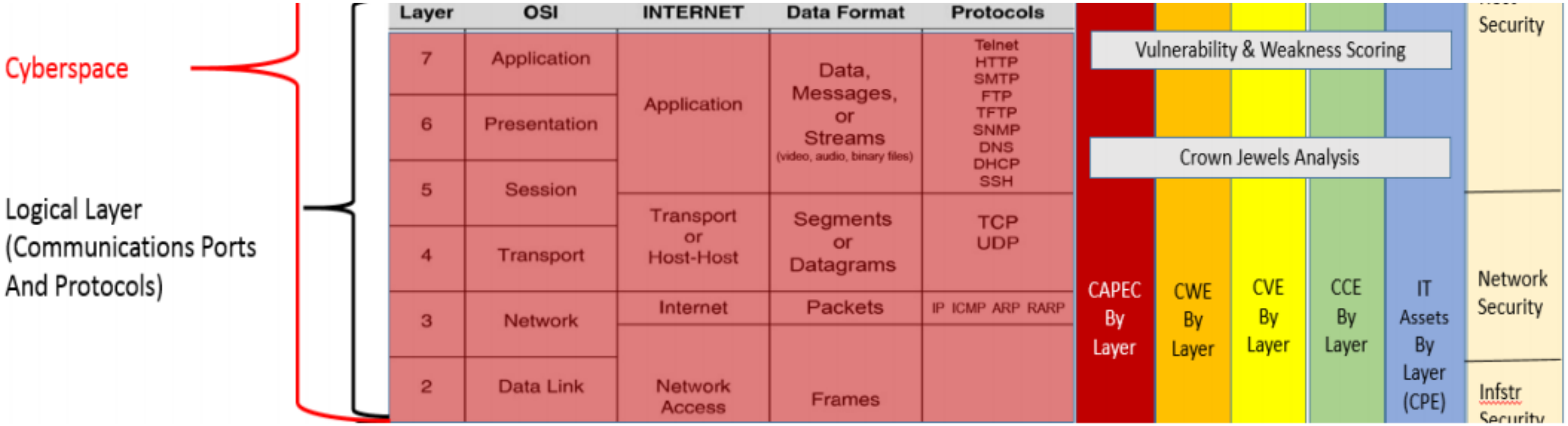
Cyber Terrain – Layers 0-1



- CAPEC-ID:455 – Malicious Logic Insertion via Inclusion of Counterfeit Hardware Components
- CAPEC-ID:453 – Malicious Logic Insertion via Counterfeit Hardware
- CAPEC-ID:547 – Physical Destruction of Device or Component
- CAPEC-ID:397 – Cloning Magnetic Strip Cards
- CAPEC-ID:391 – Bypassing Physical Locks
- CAPEC-ID:507 – Physical Theft
- CAPEC-ID:414 – Pretexting via Delivery Person
- CAPEC-ID:413 – Pretexting via Tech Support
- CAPEC-ID:407 – Social Information Gathering via Pretexting
- CAPEC-ID:406 – Social Information Gathering via Dumpster Diving

CAPEC = Common Attack Pattern Enumeration Classification (463 total attack patterns in CAPEC V2.6)
Website: http://capec.mitre.org

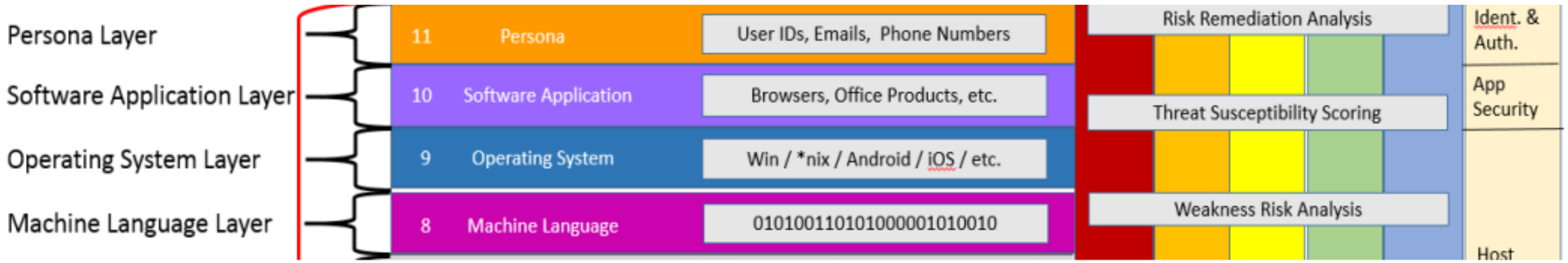
Cyber Terrain – Layers 0-1



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	

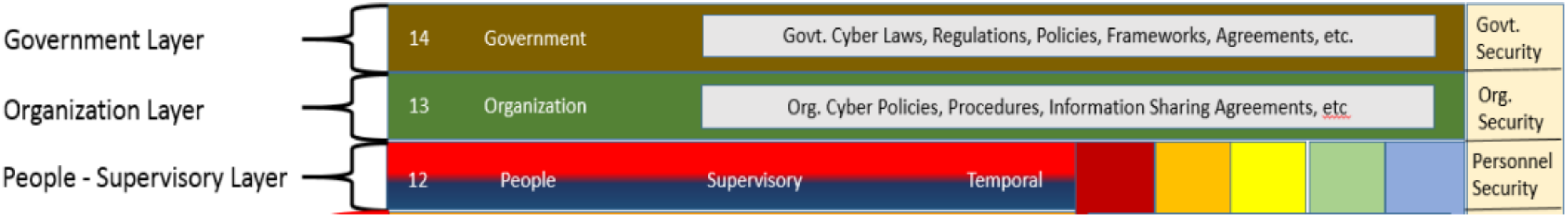
- CAPEC-ID:383 – Harvesting Usernames or UserIDs via Application API Event Monitoring (Application Layer)
- CAPEC-ID:311 – OS Fingerprinting (Network Layer, Transport Layer, & Application Layer)
- CAPEC-ID:291 – DNS Zone Transfers (Application Layer)
- CAPEC-ID:315 – TCP/IP Fingerprinting Probes (Network Layer, Transport Layer, & Application Layer)
- CAPEC-ID:310 – Scanning for Vulnerable Software (Network Layer, Transport Layer, & Application Layer)
- CAPEC-ID:311 – OS Fingerprinting (Network Layer, Transport Layer, & Application Layer)
- CAPEC-ID:309 – Network Topology Mapping (Network Layer, Transport Layer, & Application Layer)
- CAPEC-ID:293 – Traceroute Route Enumeration (Network Layer & Transport Layer)
- CAPEC-ID:316 – ICMP Fingerprinting Probes (Network Layer)

Cyber Terrain – Layers 8-11



- CAPEC-ID:37 – Lifting Data Embedded in Client Distributions
- CAPEC-ID:205 – Lifting Credential Key Material Embedded in Client
- CAPEC-ID:8 – Buffer Overflow in an API Call
- CAPEC-ID:14 – Client-side Injection-induced Buffer Overflow
- CAPEC-ID:118 – Gather Information
- CAPEC-IDS:268 – Audit Log Manipulation
- CAPEC-ID:270 – Modification of Registry Run Keys
- CAPEC-ID:17 – Accessing, Modifying or Executing Executable Files
- CAPEC-ID:69 – Target Programs with Elevated Privileges
- CAPEC-ID:76 – Manipulating Input to File System Calls
- CAPEC-ID:35 – Leverage Executable Code in Non-Executable Files
- CAPEC-ID:472 – Browser Fingerprinting
- CAPEC-ID:151 – Identity Spoofing
- CAPEC-ID:156 – Deceptive Interactions

Cyber Terrain – Layers 12-14



Government Layer

14 Government

Govt. Cyber Laws, Regulations, Policies, Frameworks, Agreements, etc.

Govt. Security

Organization Layer

13 Organization

Org. Cyber Policies, Procedures, Information Sharing Agreements, etc

Org. Security

People - Supervisory Layer

12 People Supervisory Temporal

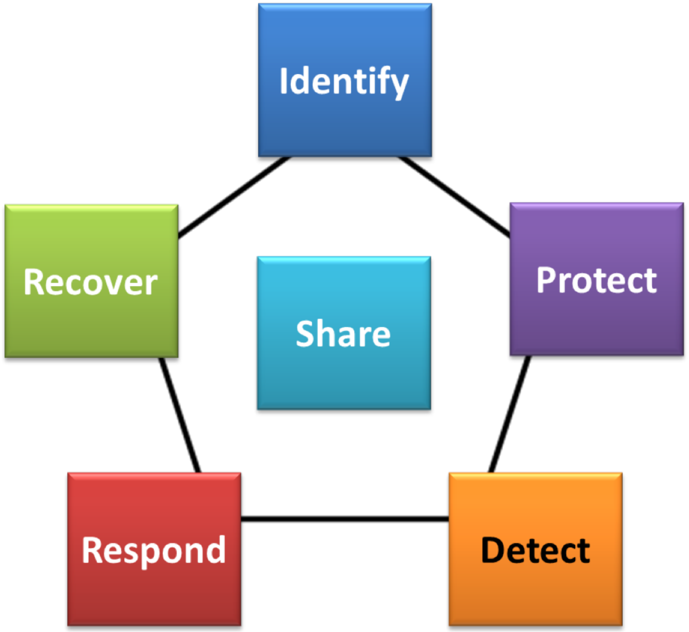
Personnel Security

- CAPEC-ID:404 – Social Information Gathering Attacks
- CAPEC-ID:410 – Information Elicitation via Social Engineering
- CAPEC-ID:416 – Target Influence via Social Engineering
- CAPEC-ID:527 – Manipulate System Users
- CAPEC-ID:156 – Deceptive Interactions
- CAPEC-ID:98 – Phishing
- CAPEC-ID:163 – Spear Phishing
- CAPEC-ID:164 – Mobile Phishing (aka MobPhishing)

Global Cyber Security Ecosystem

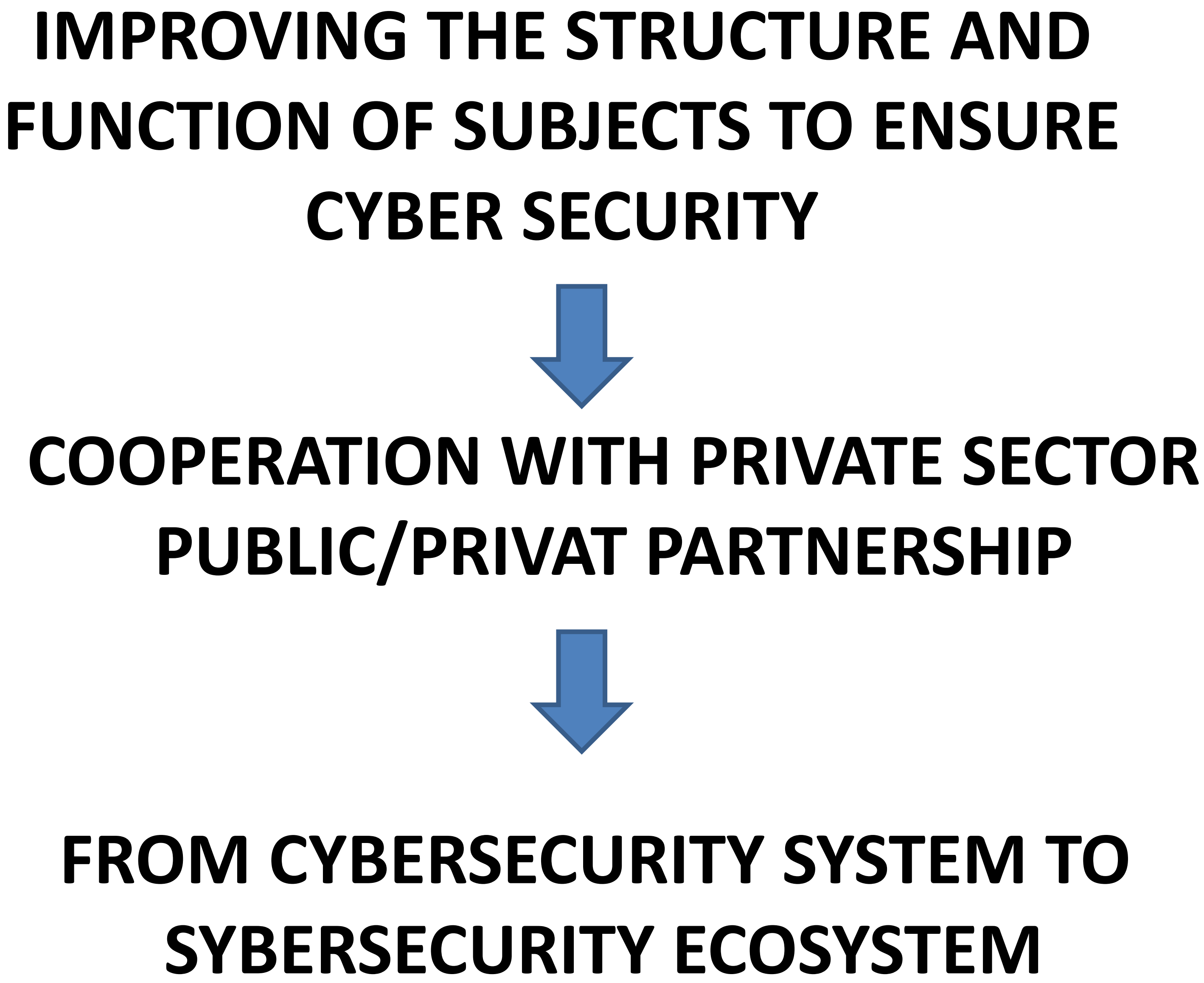
ETSI TR 103 306 V0.5.1 (2015-02)

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.

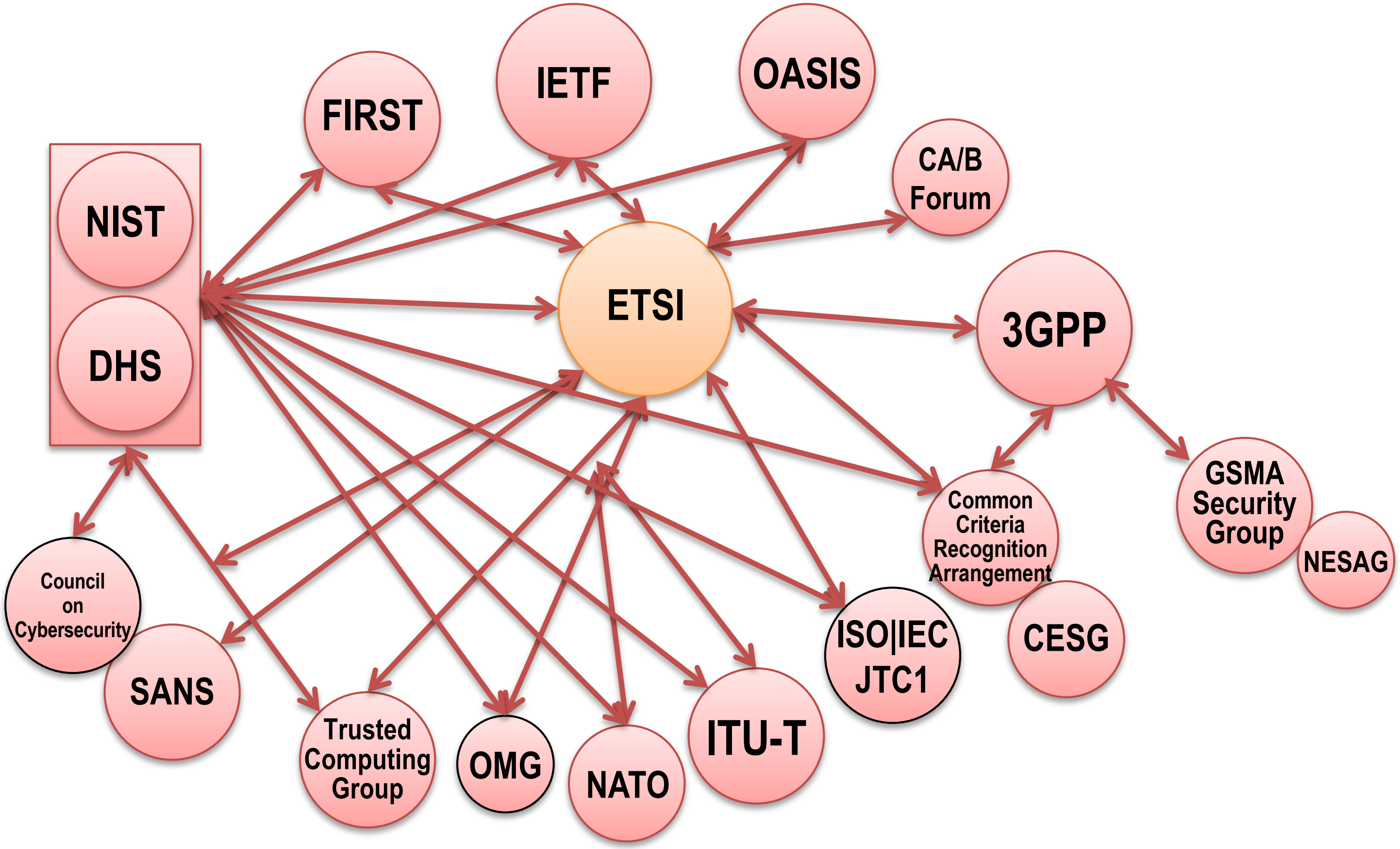


IMPROVING THE STRUCTURE AND FUNCTION OF SUBJECTS TO ENSURE CYBER SECURITY

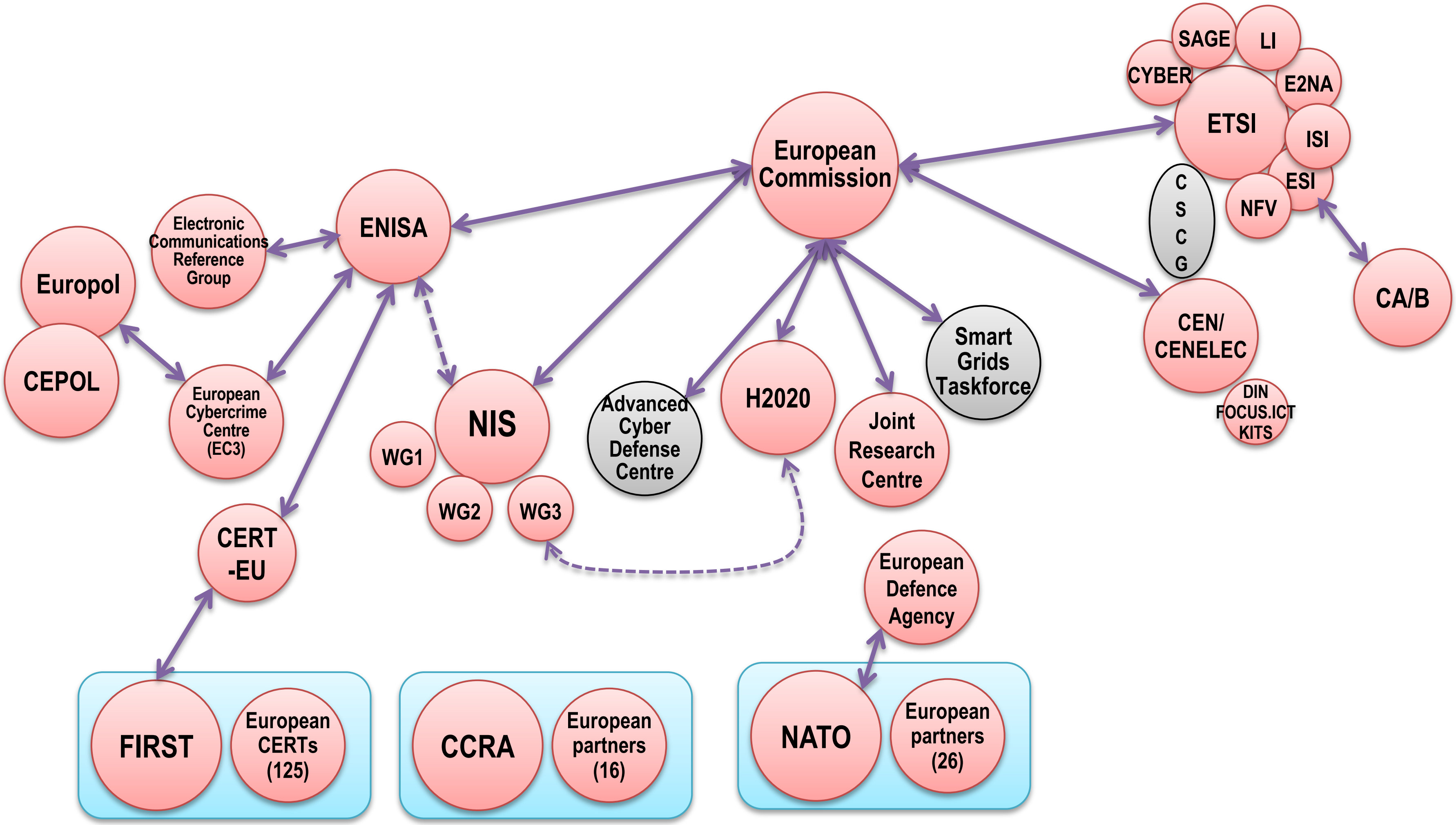
COOPERATION WITH PRIVATE SECTOR PUBLIC/PRIVAT PARTNERSHIP

FROM CYBERSECURITY SYSTEM TO SYBERSECURITY ECOSYSTEM

EVOLVING GLOBAL CYBER SECURITY ECOSYSTEM



EUROPEAN CYBER SECURITY TECHNICAL ECOSYSTEM



European Commission

ETSI

SAGE

LI

CYBER

E2NA

ISI

ESI

NFV

CSCG

CA/B

CEN/ CENELEC

DIN FOCUS.ICT KITS

Smart Grids Taskforce

Joint Research Centre

H2020

Advanced Cyber Defense Centre

ENISA

Electronic Communications Reference Group

Europol

CEPOL

European Cybercrime Centre (EC3)

NIS

WG1

WG2

WG3

CERT -EU

European Defence Agency

FIRST

European CERTs (125)

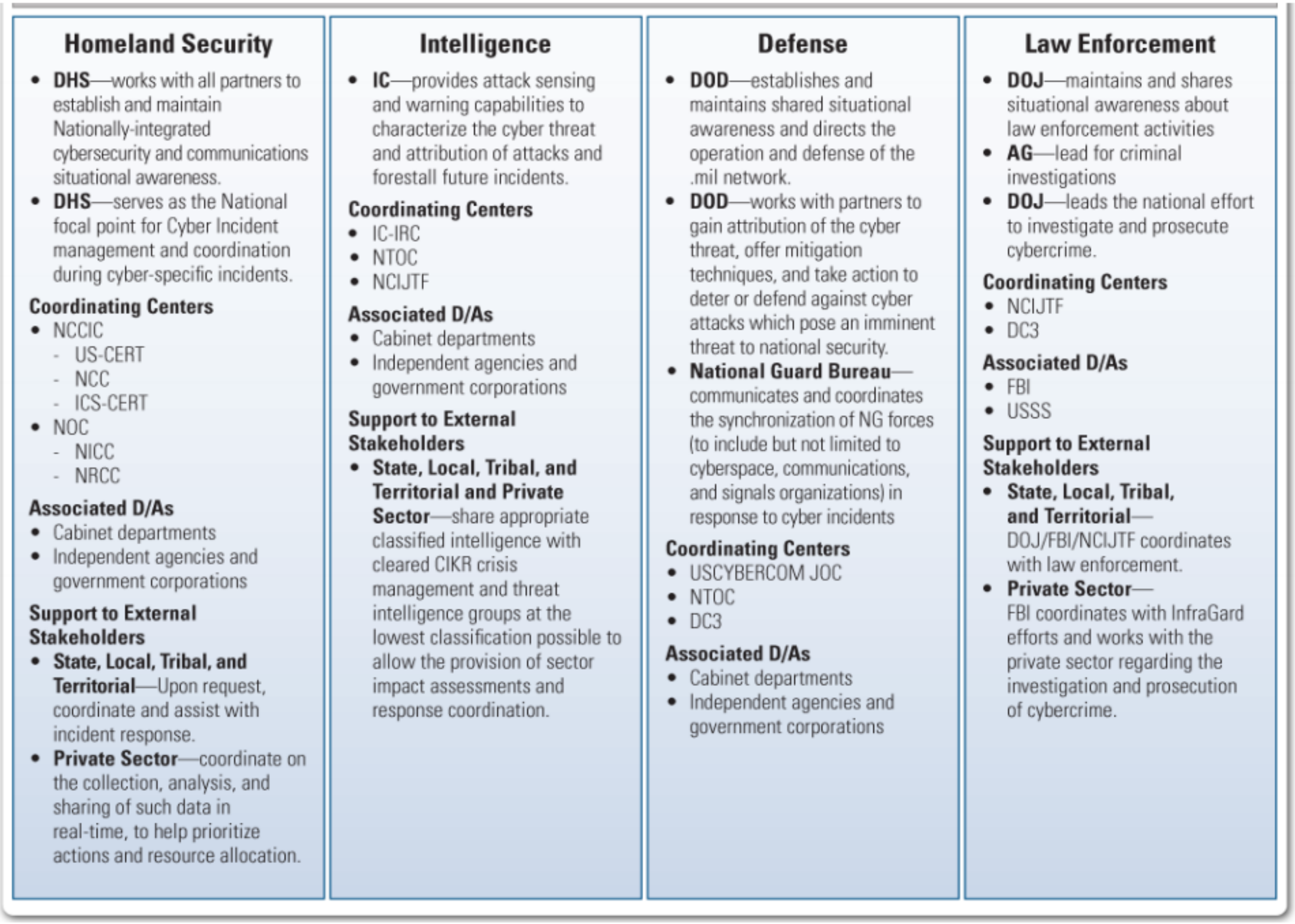
CCRA

European partners (16)

NATO

European partners (26)

CYBERSECURTY SYSTEM OF USA



Homeland Security

- **DHS**—works with all partners to establish and maintain Nationally-integrated cybersecurity and communications situational awareness.
- **DHS**—serves as the National focal point for Cyber Incident management and coordination during cyber-specific incidents.

Coordinating Centers

- NCCIC
  - US-CERT
  - NCC
  - ICS-CERT
- NOC
  - NICC
  - NRCC

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to External Stakeholders

- **State, Local, Tribal, and Territorial**—Upon request, coordinate and assist with incident response.
- **Private Sector**—coordinate on the collection, analysis, and sharing of such data in real-time, to help prioritize actions and resource allocation.

Intelligence

- **IC**—provides attack sensing and warning capabilities to characterize the cyber threat and attribution of attacks and forestall future incidents.

Coordinating Centers

- IC-IRC
- NTOC
- NCIJTF

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Support to External Stakeholders

- **State, Local, Tribal, and Territorial and Private Sector**—share appropriate classified intelligence with cleared CIKR crisis management and threat intelligence groups at the lowest classification possible to allow the provision of sector impact assessments and response coordination.

Defense

- **DOD**—establishes and maintains shared situational awareness and directs the operation and defense of the .mil network.
- **DOD**—works with partners to gain attribution of the cyber threat, offer mitigation techniques, and take action to deter or defend against cyber attacks which pose an imminent threat to national security.
- **National Guard Bureau**—communicates and coordinates the synchronization of NG forces (to include but not limited to cyberspace, communications, and signals organizations) in response to cyber incidents

Coordinating Centers

- USCYBERCOM JOC
- NTOC
- DC3

Associated D/As

- Cabinet departments
- Independent agencies and government corporations

Law Enforcement

- **DOJ**—maintains and shares situational awareness about law enforcement activities
- **AG**—lead for criminal investigations
- **DOJ**—leads the national effort to investigate and prosecute cybercrime.

Coordinating Centers

- NCIJTF
- DC3

Associated D/As

- FBI
- USSS

Support to External Stakeholders

- **State, Local, Tribal, and Territorial**—DOJ/FBI/NCIJTF coordinates with law enforcement.
- **Private Sector**—FBI coordinates with InfraGard efforts and works with the private sector regarding the investigation and prosecution of cybercrime.

UNIQUELY POSITIONED AMONG FEDERAL CYBER CENTERS

National Cyber Investigative Joint Task Force (NCI-JTF)

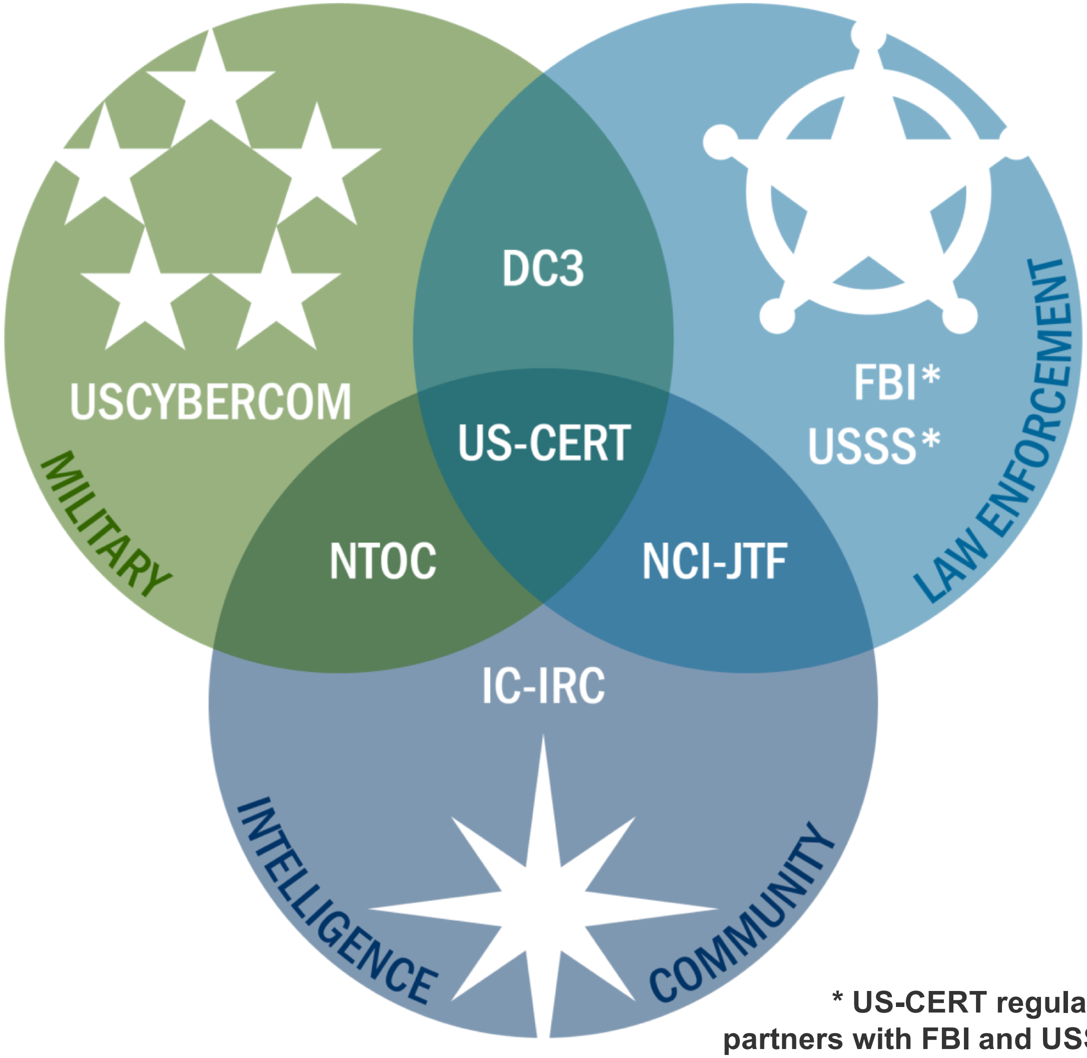
Department of Defense Cyber Crime Center (DC3)

US Cyber Command (USCYBERCOM)

US Computer Emergency Readiness Team (US-CERT)

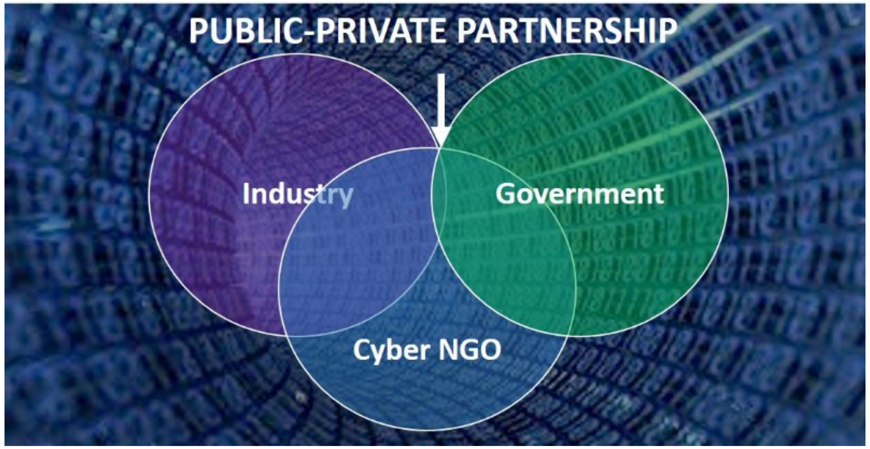
NSA/Central Security Service (CSS) Threat Operations Center (NTOC)

Intelligence Community Incident Response Center (IC-IRC)



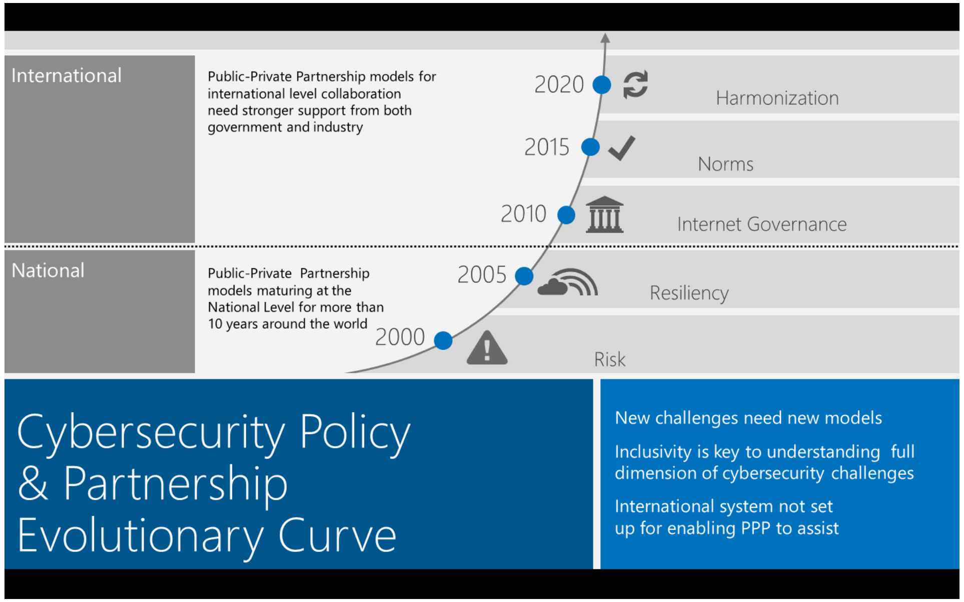
* US-CERT regularly partners with FBI and USSS teams in the same capacity as those from the cyber centers

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
National
2020
Harmonization
2015
Norms
2010
Internet Governance
2005
Resiliency
2000
Risk

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

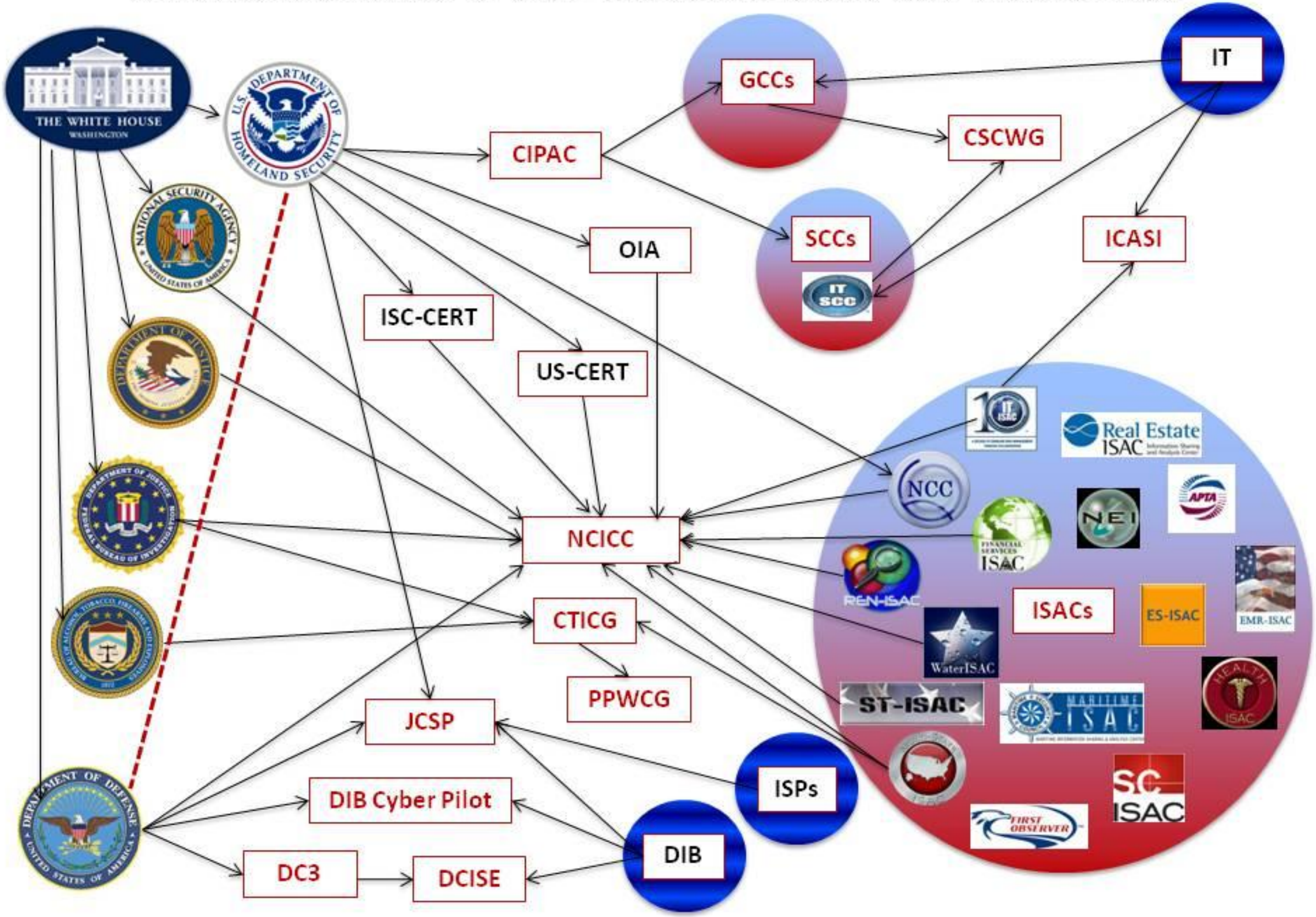
Inclusivity is key to understanding full dimension of cybersecurity challenges

International system not set up for enabling PPP to assist

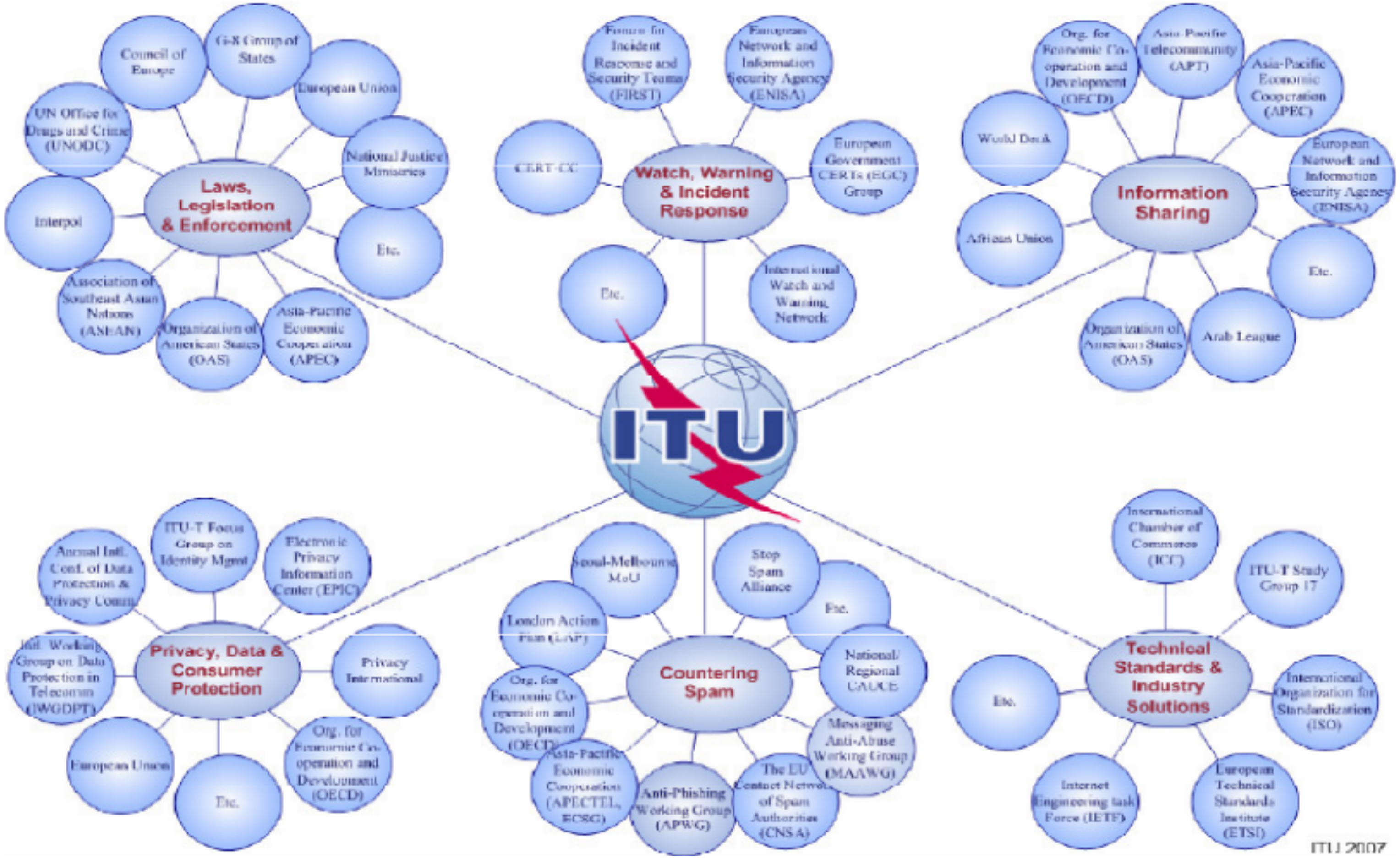
Today industry creates and operates most of the infrastructure that enables cyberspace. Industry continues to innovate and build best practices and technical cybersecurity norms including: vulnerability disclosure management, secure development, security incident response, and risk management. Therefore, 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



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?