Cyber Security
From Regulations\Policies to Practice

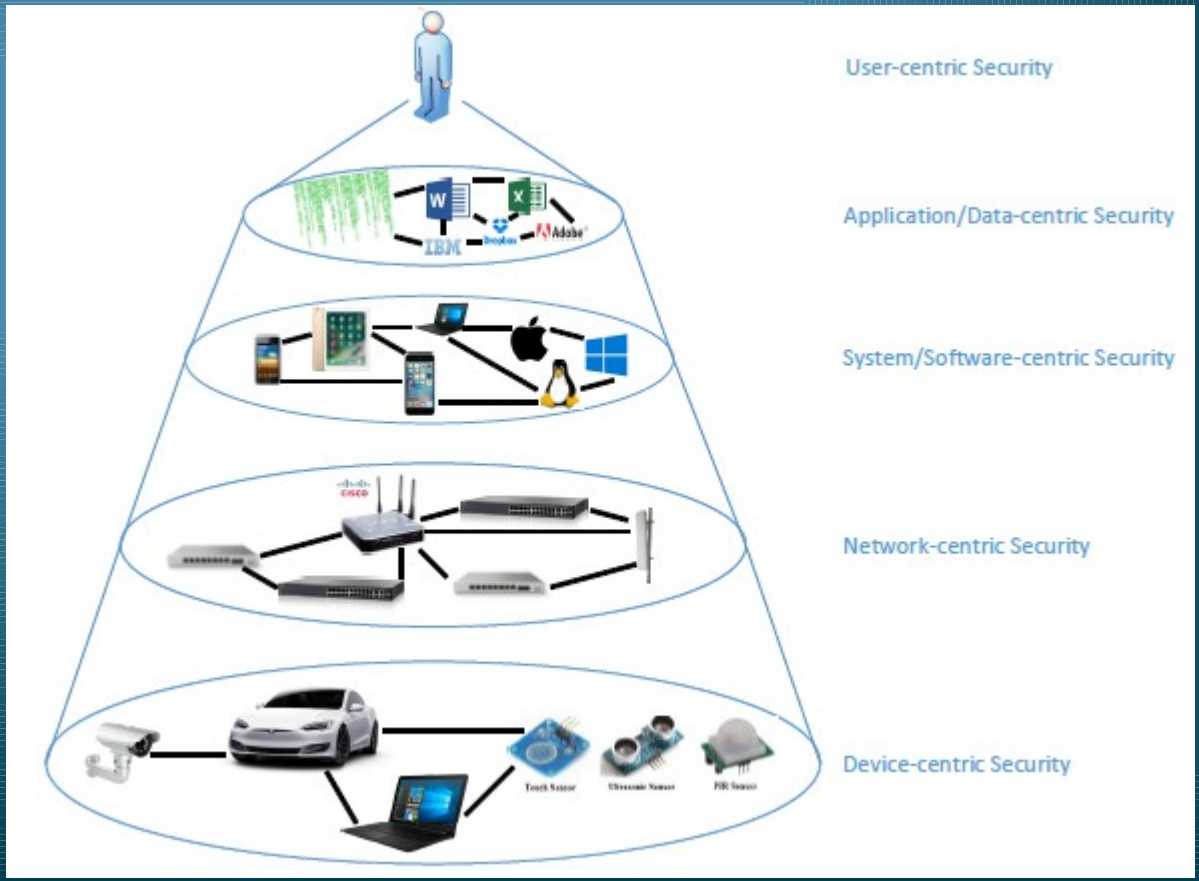
Dr. Leandros Maglaras
Head of the National Cyber Security Authority of Greece
General Secretariat of Digital Policy
Ministry of Digital Policy, Telecommunications and Media

ENISA – FORTH Summer School 2018 on Network and Information Security
24-28/09 Heraklion, Crete, Greece

Layers of Cyber Security

Target environment of the future :

- **complex interconnected systems**
- **highly heterogeneous**
- **highly dynamic environments**
- **highly mobile**



Lifecycle of Cybersecurity

Proactive measures to identify potential attackers, intentions and methods

Prediction

Protection

Security measures and controls to protect from, deter and stop attacks as well minimize the impact of a compromise

Detection

Process of monitoring to identify intrusions and attacks

Reaction

Processes and methods to investigate intrusions and respond to a compromise

Cyber Threat Intelligence

Risk Management for cyber security

Cyber Risk is Unpredictable

- Vulnerabilities
- Intentions of threats
- Budget

Failure is inevitable (Perrow's)

- Interactive Complexity
- Tight coupling

	Good for
Component-driven methods	• Analysing the risks faced by individual technical components. • Deconstructing less complex systems, with well-understood connections between component parts. • Working at levels of abstraction where a system's physical function has already been agreed amongst stakeholders.
System-driven methods	• Exploring security breaches which emerge out of the complex interaction of many parts of your system. • Establishing system security requirements before you have decided on the system's exact physical design. • Bringing together multiple stakeholders' views of what a system should and should not do (eg safety, security, legal views). • Analysing security breaches which cannot be tracked back to a single point of failure.

COBIT 5
AN ISACA® FRAMEWORK

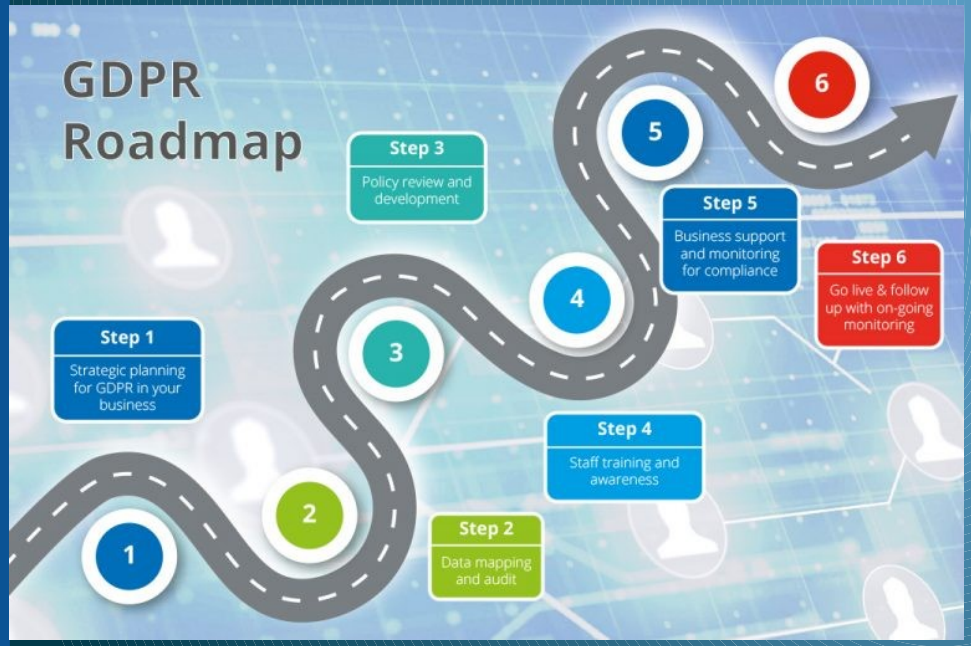
ISO 27001

NIST CYBERSECURITY FRAMEWORK (CSF)

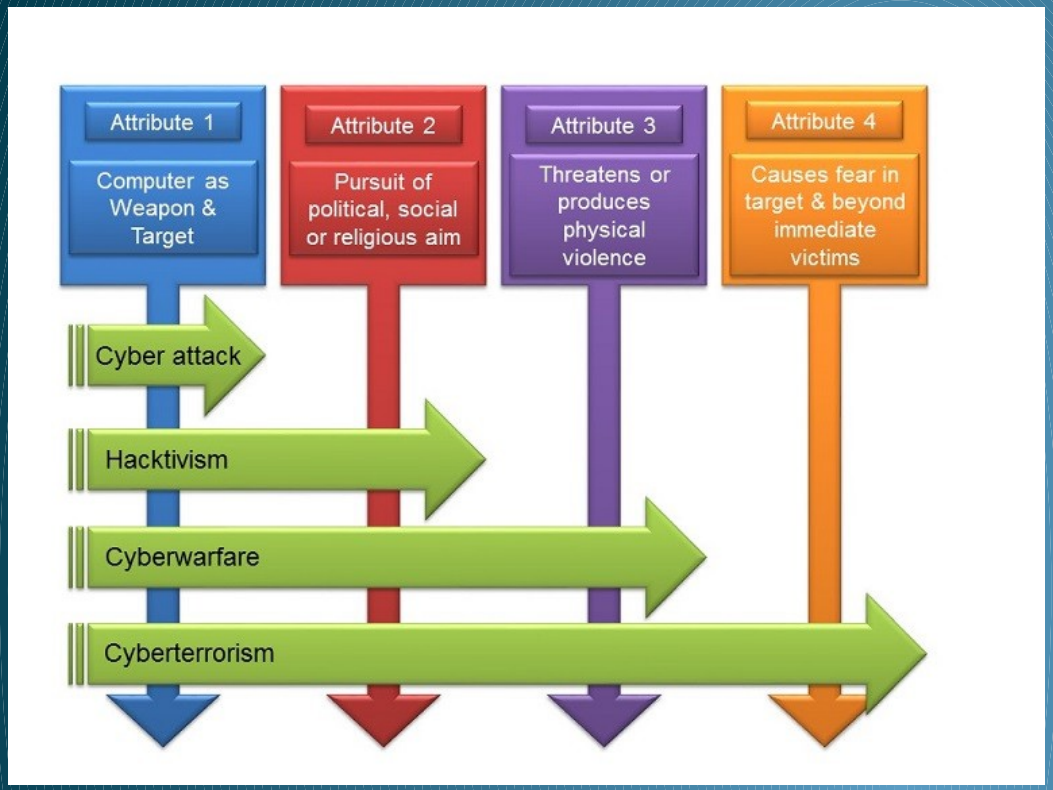
IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

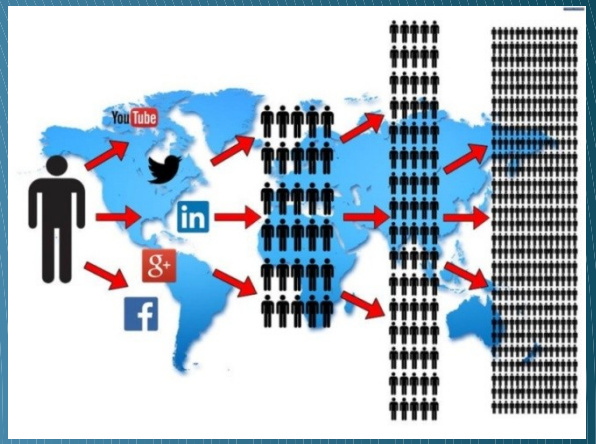
Cybersecurity modern Landscape

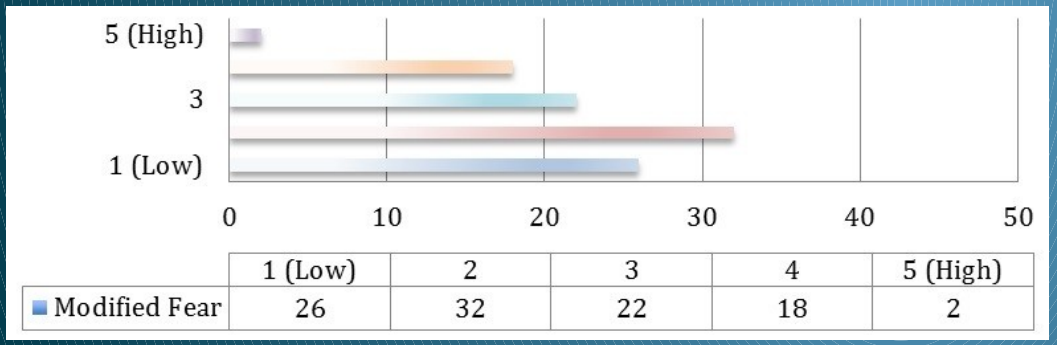
- NIS directive - security and incident notification (Operators of Essential Services) – 9th of May
- GDPR – privacy and incident notification (any company that offers goods/services (paid or for free) or monitoring the behaviour of individuals in the EU – 25th of May
- E-privacy - privacy rules for all electronic communications; “cookie law” (also covers whatsup, Facebook Messenger and Skype)



Hybrid war - Cyber Terrorism



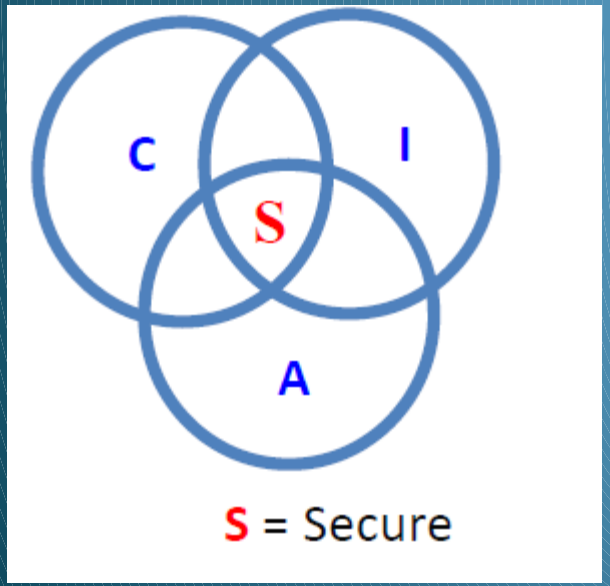




Nicholas Ayres, Leandros A. Maglaras, "Cyberterrorism targeting general public through social media", Security and Communication Networks (WILEY), Volume 9, Issue 15, October 2016, pp: 2864-2875

NIS directive – OES

- Energy(Electricity, Oil, Gas)
- Healthcare
- Banking
- Transport
- Drinking water supply and distribution
- Digital infrastructure sectors



Impact on local, regional, national or global economy

Attack vectors similar to IT
- Reconnaissance
- Malware delivery and propagation
- Spear phishing
- Remote access

Industrial Control Systems

European Electrical Grid

SCADA networks are everywhere around us: Electric power generation, transmission and distribution, Water and sewage, Buildings, facilities and environments, Manufacturing, Mass transit, Traffic signals

Our society needs to keep alive these services to well function… to provide our European way of life.

European Natural Gas Grid

Industrial Control Systems

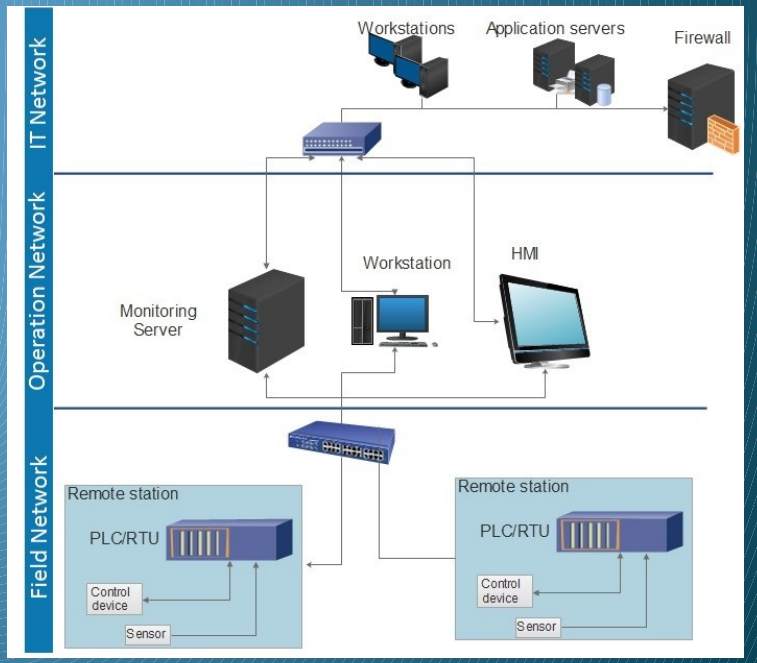
An ICS system usually consists of the following subsystems:

- **Remote terminal units (RTUs)**
- **Programmable logic controller (PLCs)**
- **A human–machine interface or HMI**
- **Supervisory computer system**
- **Network infrastructure**

Once isolated – increased connectivity

Advantages
- Real time monitoring
- Peer to peer communications
- Concurrency
- Redundancy
- Qos

New Threats – 11 connections



Vulnerabilities - Threats

- Diversity of vendors
- Widening of networks
- Aging of equipment
- Data simplicity
- Real-time processing
- Linkage with information systems
- Generalization of equipment
- IOT

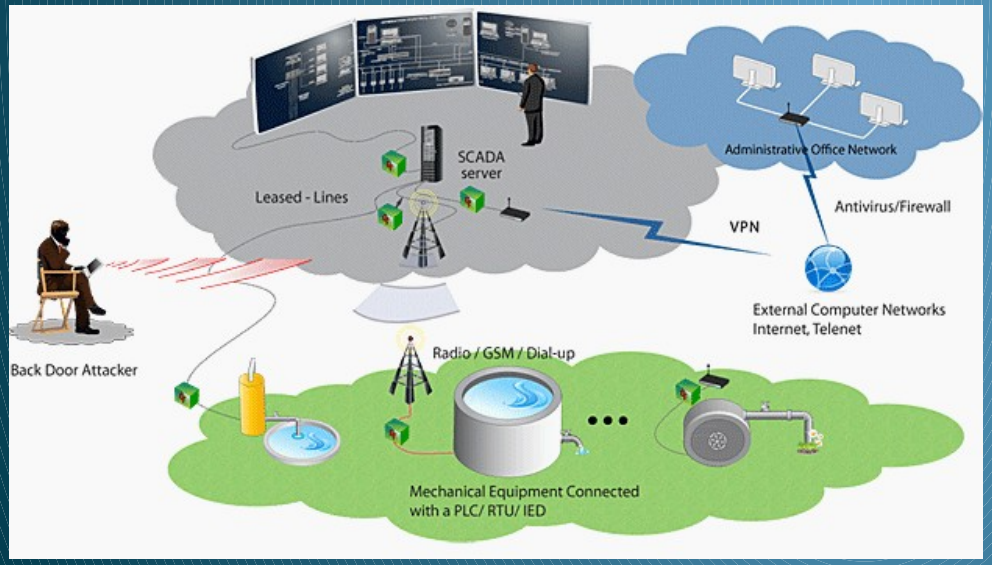


Photo by Cryptango - securing industrial communications

Threats:

Internal

- Non malicious
- Malicious

External

- Opportunistic
- Deliberate

Protection of critical information assets

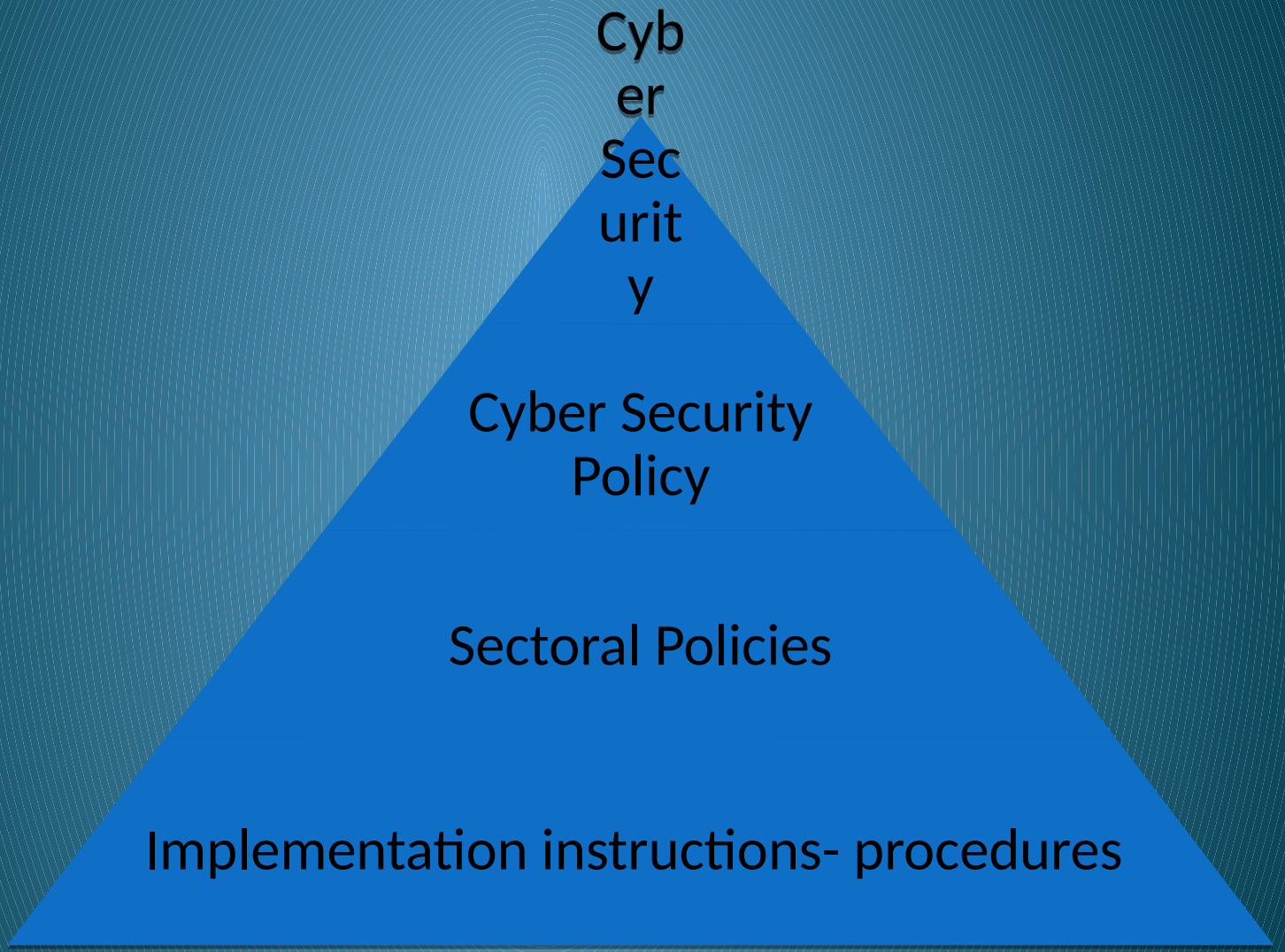
- **Cyber Security Policies**
  1. Policy upkeep, refinement of policy, and compliance
  2. Cyber security countermeasures
  3. Cyber security technologies
  4. Incident response
  5. Forensics
  6. Access control
  7. Physical security
  8. Patches and upgrading
- **Antivirus/ antimalware**
- **Firewalls**
- **Intrusion Detection System (IDS)**
  Intrusion Prevention System (IPS)
- **Unified Threat management (UTM)**
- **Online Vulnerability Map Tool**

Cyber Security objectives

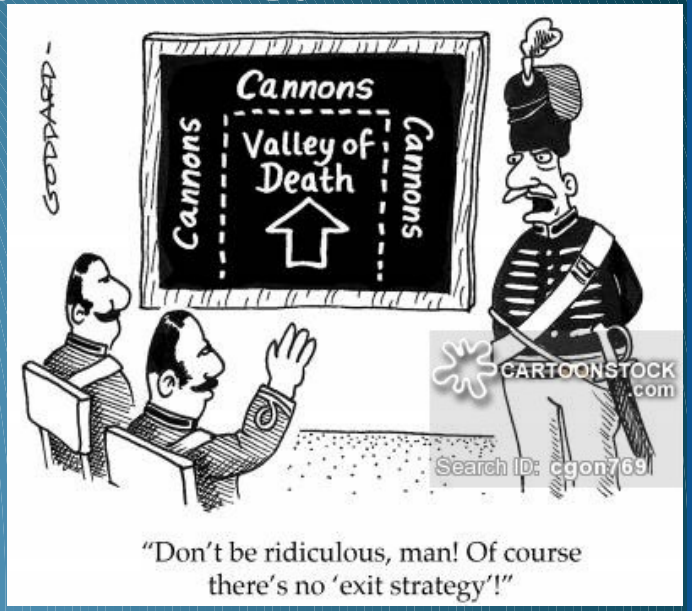
- Development and establishment of a secure and resilient cyberspace
  - in accordance with national, EU and international rules
  - citizens, public and private sector stakeholders are active contributors
  - protect human rights, freedom, justice and transparency
- Continuous improvement of capabilities
  - Training
  - Education
  - Technologies
- Institutional shielding of the national cyber security framework
  - International laws
  - EU regulation and directives
  - National legistation

Cyber security implementation steps

Why;
What;
Who;
How;



Greece National Cyber Security Strategy

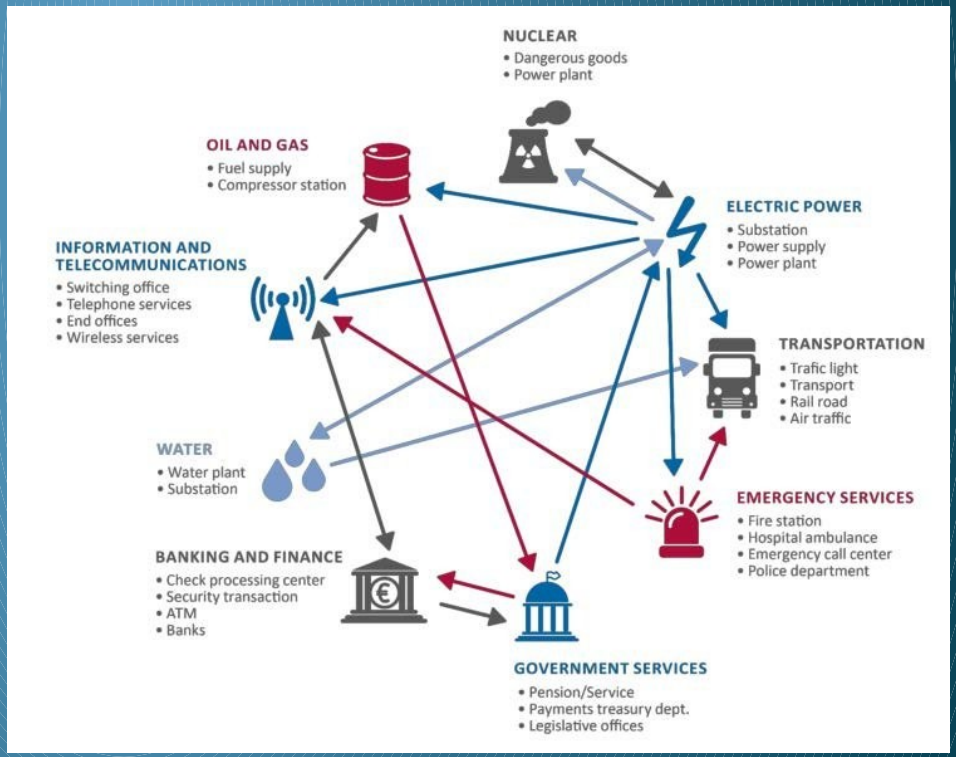


"Don't be ridiculous, man! Of course there's no 'exit strategy'!"

- Define objectives
- Define stakeholders
- Define Critical Infrastructures
- Determine basic security requirements
- Cyber security incident handling
- National Cyberspace Contingency Plan
- National preparedness exercises
- User-citizen awareness
- Reliable information exchange mechanisms
- Record and improve the existing institutional framework
- Support of research and development programmes and academic educational programmes
- Cooperation at international level
- Evaluation and revision of the National Strategy

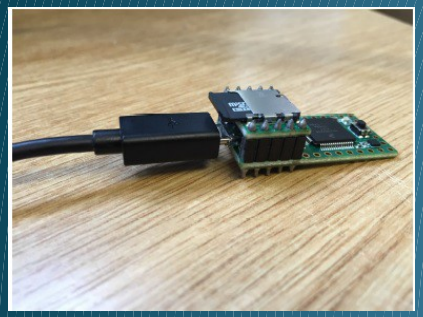
Security consists of….

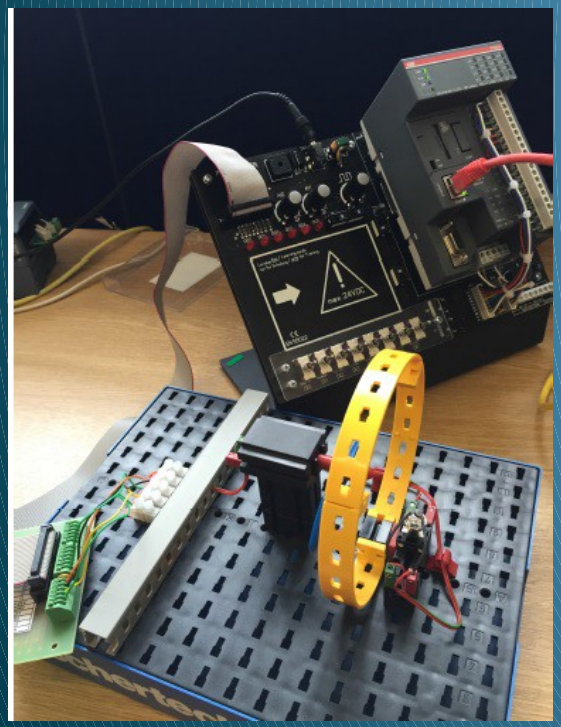
+ Interdepedencies



+ Trust

Are policies enough?

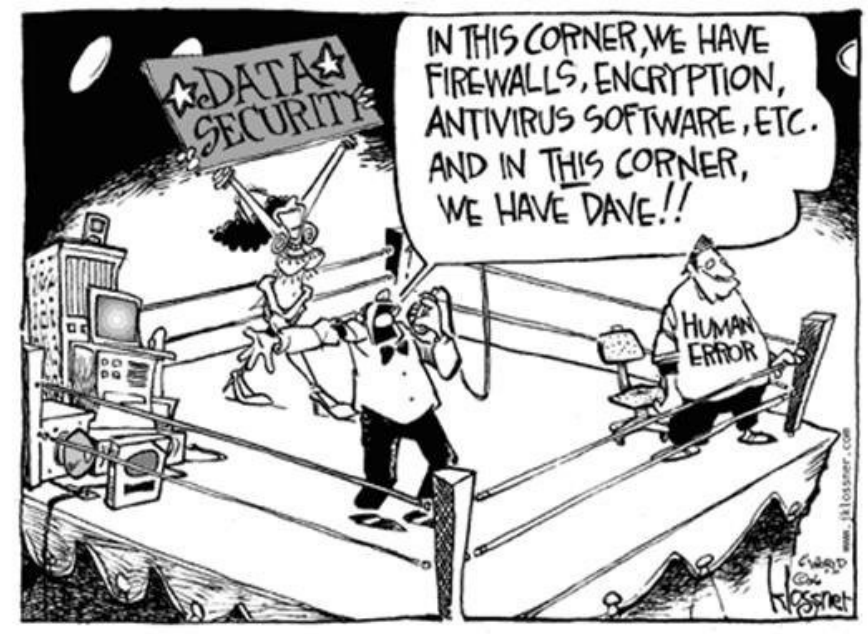


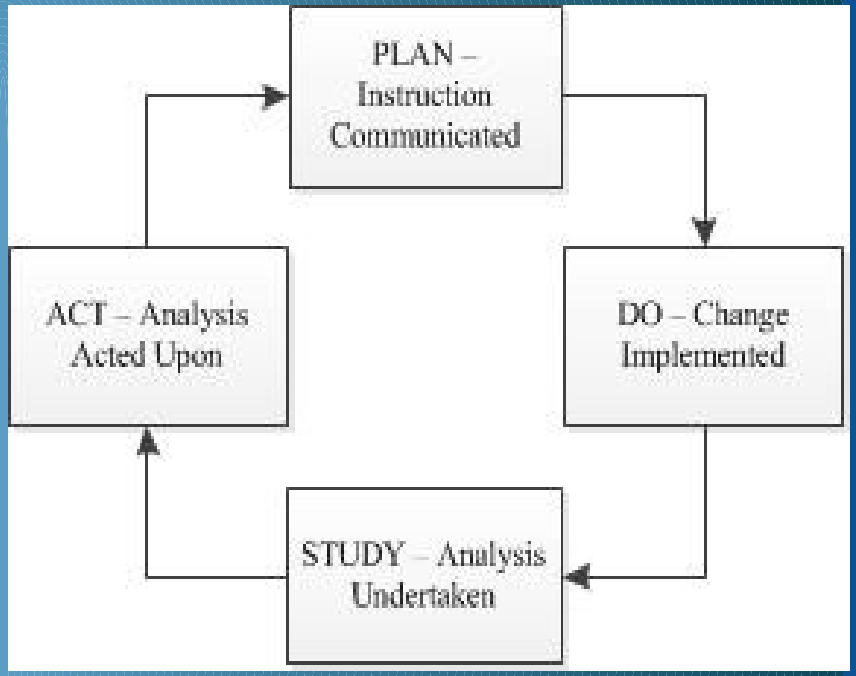



```
def pkt_send():
    mysocket = socket.socket()
    mysocket.connect
        (('192.168.0.10',1201))
    myStream = StreamSocket(mysocket)
    req = Raw(load="\xbb\xbb\x00\x00
        ......")
    req1 = Raw(load="\xbb\xbb\x00\x00
        .....")
    req2 = Raw(load="\xbb\xbb\x00\x00
        .....")
    req3 = Raw(load="\xbb\xbb\x00\x00
        .....")
    myStream.send(req)
    time.sleep(0.1)
    myStream.send(req1)
    time.sleep(0.1)
    myStream.send(req2)
    time.sleep(1)
    myStream.send(req3)
    time.sleep(0.1)
    mysocket.close()
pkt_send()
```

Are technologies enough?

50% of the incidents are due to human error





Technology-related breaches vs human error

Need of new techniques for assessing human errors in IT security incidents (HEART-IS)

Mark Evans, Leandros Maglaras, Ying He, Helge Janicke, "Human behavior as an aspect of Cyber Security Assurance", Security and Communication Networks (WILEY), Volume 9, Issue 17, November 2016

Mark Evans, Ying He, Leandros Maglaras, Helge Janicke, “HEART-IS: A Novel Technique for Evaluating Human Error-Related Information Security Incidents”, Elsevier Computers and Security, Accepted September 2018

Human Error Related Security Incident Definition

‘an ‘active failure’ by a person (the threat) performing an ‘intentional action’ resulting in the failure to complete a task as intended or achieve the desired outcome due to the exploitation of a ‘latent condition’ (the vulnerability).

Leading to a compromise, or breach, of information confidentiality, integrity or availability or associated law through the failure of technical or organisational safeguards.

Causing disruption to business operations or causing harm or distress to individuals including breaches of privacy.

Are procedures enough?

1. **Awareness (APTs)**
2. **Training**
3. **Exercises**
   Help test cooperation in the country
   Help test cooperation among countries

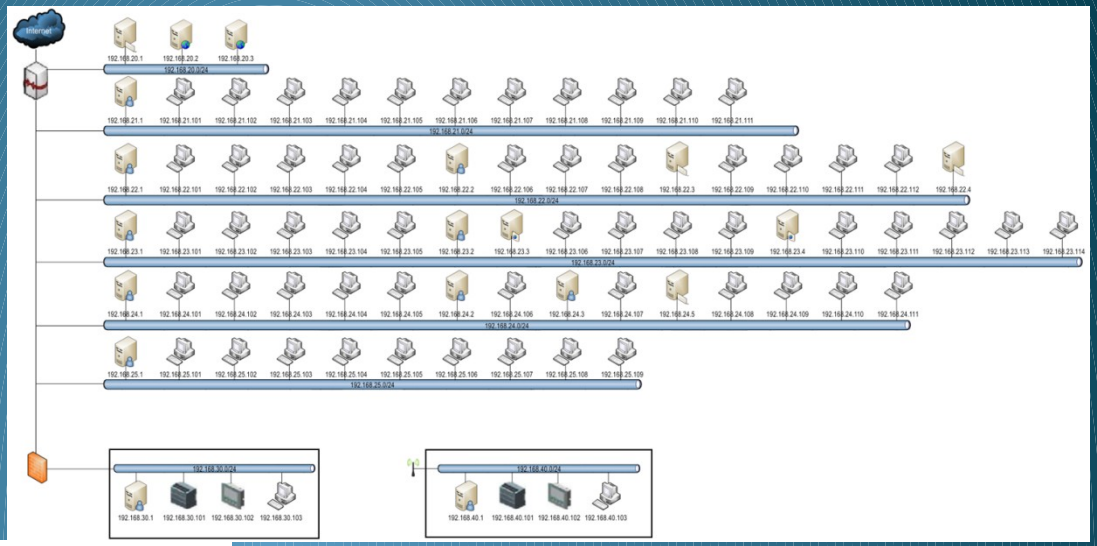
Awareness campaigns

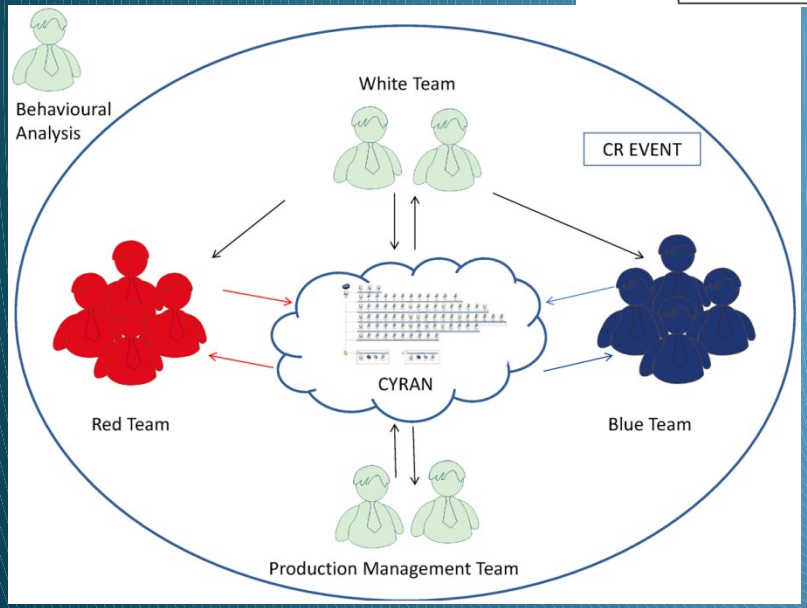
- Focus on lectures or presentations
- Deliver a lot of information in limited time
- Quality of information is important but not sufficient
- Long term perspective of the audience
- **Experiential learning ->active engagement, failure helps**

SCIPS - Simulated Critical Infrastructure Protection Scenarios

Allan Cook, Richard Smith, Leandros Maglaras, Helge Janicke, "SCIPS: Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control Systems", International Journal of Cyber Warfare and Terrorism (IGI-Global), Volume 7, Issue 2, May 2017, DOI: 10.4018/IJCWT.2017040101

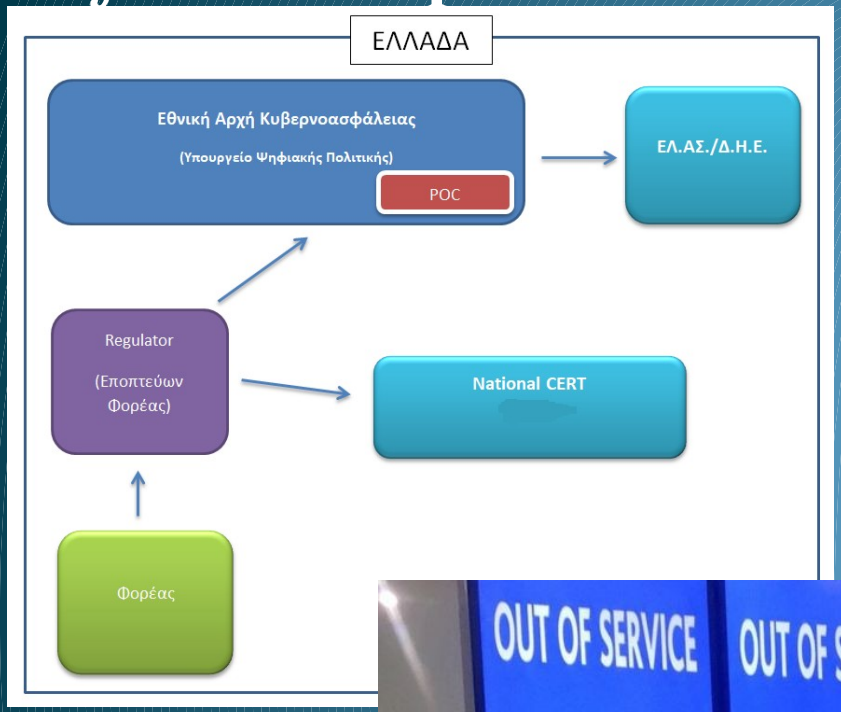
CYRAN: A Hybrid Cyber Range for Testing Security on ICS/SCADA Systems

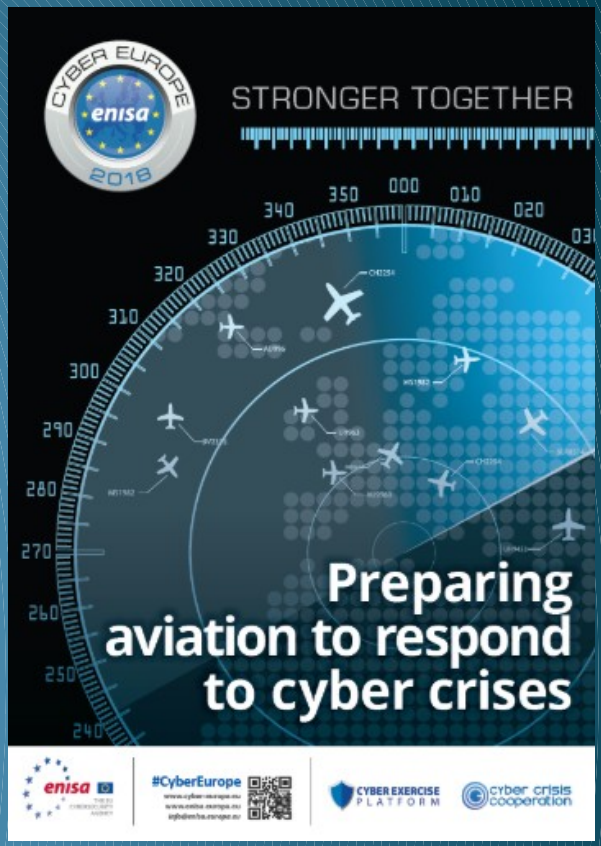


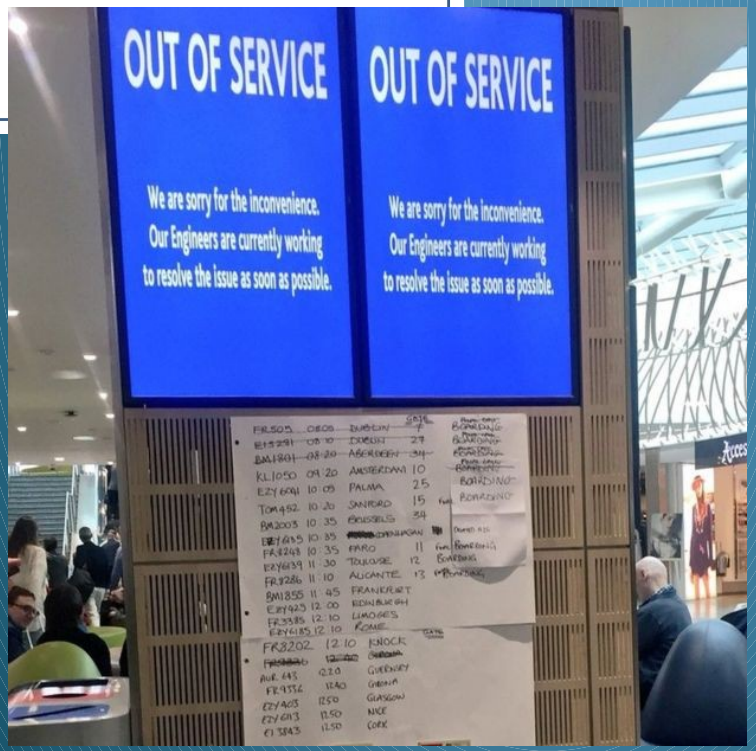


Bil Hallaq, Andrew Nickolson, Richard Smith, Leandros Maglaras, Helge Janicke, Kevin Jones, "CYRAN, a Hybrid Cyber Range for testing security on ICS/SCADA systems", Chapter in Security Solutions and Applied Cryptography in Smart Grid Communications (Mohamed Amine Ferrag, Ahmed Ahmim), IGI Global, November 2016, DOI: 10.4018/978-1-5225-1829-7.ch012

Cyber Europe 2018







Trust

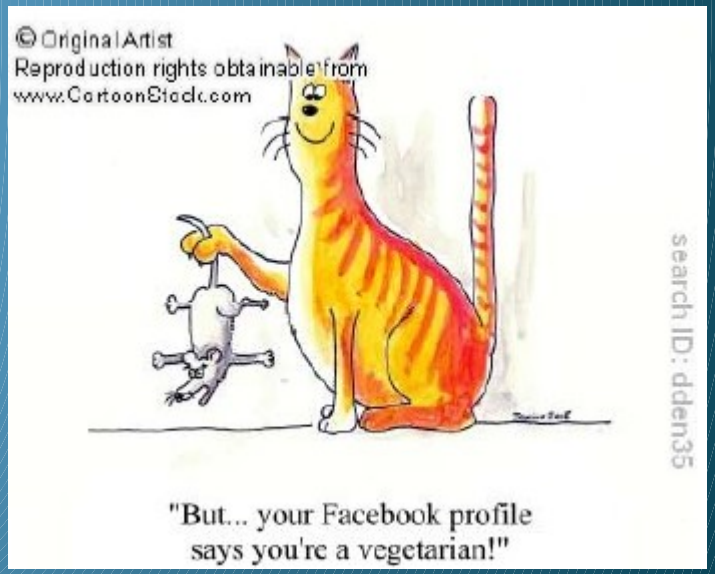
1. Cooperation group EU
   I. Identification of OESs
   II. Consultation in cases with cross-border impact
   III. Security measures
   IV. Notification requirements, procedures, format
   V. Elections
   VI. Large scale incidents
   VII. Capacity building
2. CSIRT network
3. SPoC
4. CBMs

Trust

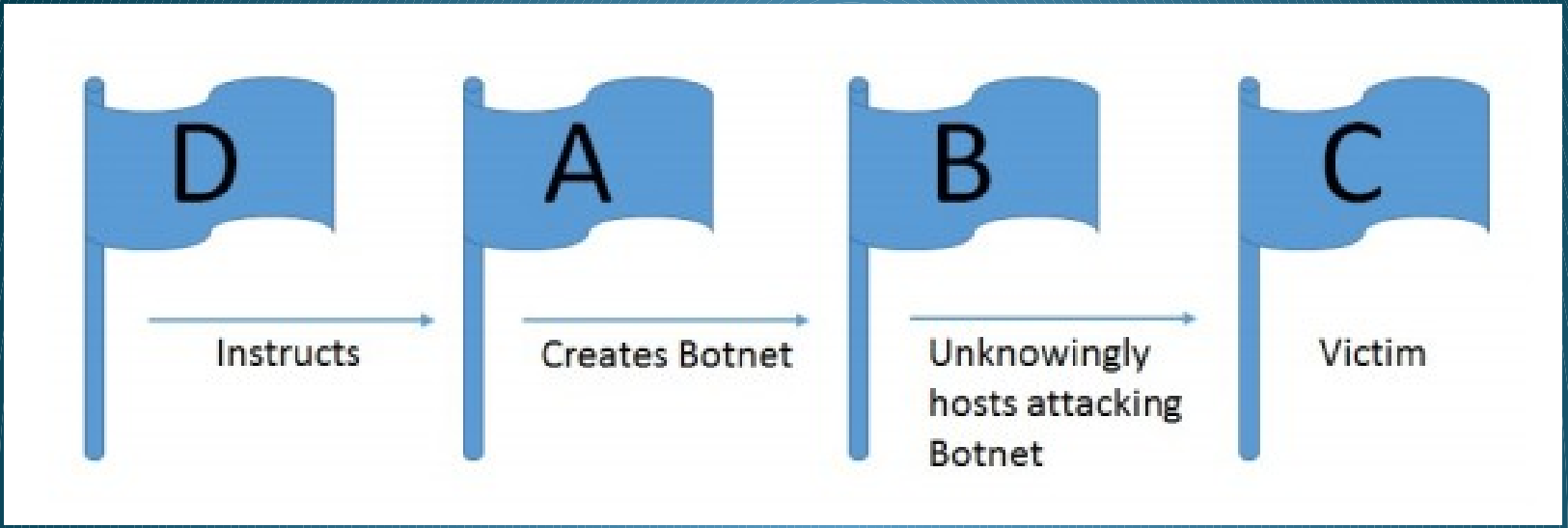
CBMs provide practical tools to manage acceptable norms of state behaviour expectations

CBMs facilitate nations cooperation, for example through establishing channels of communication, information exchange on threats, exchanging best practices, raising awareness and practical cooperation

1. **Unites Nations**
2. **OSCE**
3. **EE**



Attribution of attacks – assigning responsibility



An illustration of the complexity of nation-state responsibility in attribution (state D instructs a group in state A to assimilate computers in state B in order to attack state C)

1. **Tallinn Manual**
2. **Tallinn 2.0 (focus on** cyber "operations" as opposed to cyber "conflict" from the original Tallinn Manual)

Cook, A., Nicholson, A., Janicke, H., Maglaras, L., & Smith, R. (2016). Attribution of Cyber Attacks on Industrial Control Systems.

CBMs best practices

- Broadening Cooperation Through Capacity-Building
- Assistance in establishing national CERTs
- Bilateral team-to-team cooperation
- Council of Europe Convention on Cybercrime (Treaty No. 85)
- Cooperation groups - network of CSIRTs (EE)

EU response, USA response

Cyber diplomacy toolbox from EE

Preventive, resolving measures and attribution

Deterring effect of a swift response

Assign responsibility for malicious cyber activities

Impose measures

Cyber deterrence USA

A Policy with clear criteria – communicated publicly

A range of consequences – swift, costly transparent

Building partnerships

The need for cyber peace keeping

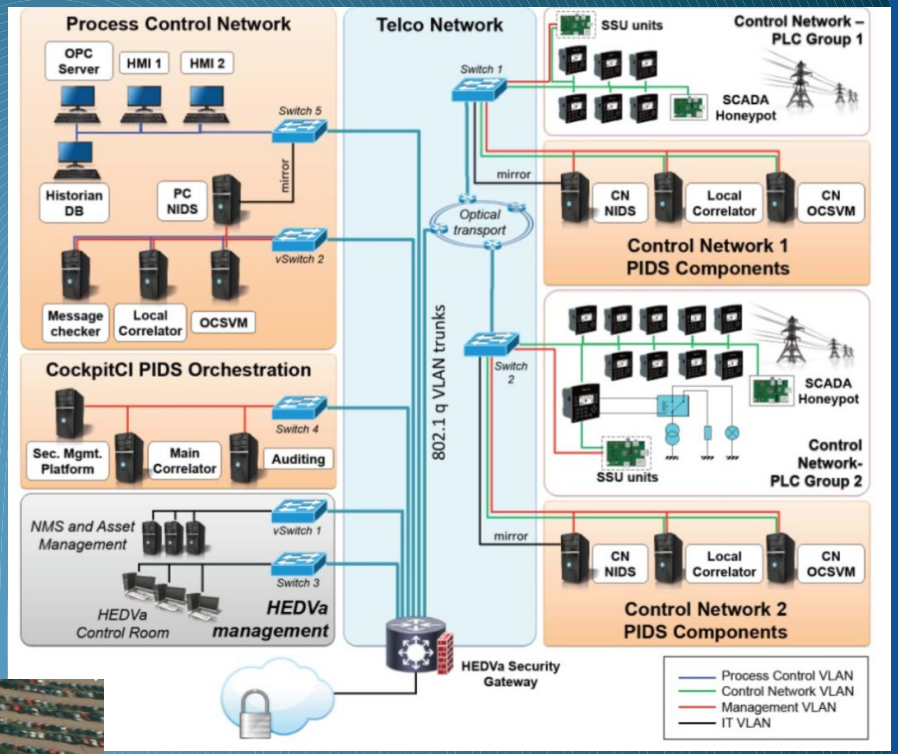
- Securing the required cyber expertise will likely be the biggest obstacle towards cyber peacekeeping.
- Cyber fits easily into existing structures and processes.
- Cyber OMR will bring most value at CNI, with a focus on protection of civilians and state stability
- Technical obstacles towards monitoring CNI are being broken down as new products and tools come to market
- Use of a virtual collaborative environment : transparency, ease of collaboration, information sharing and keeping capability at home

Robinson M., Jones K., Janicke H., Maglaras L., An introduction to cyber peacekeeping, Journal of Network and Computer Applications, Volume 114, 2018, Pages 70-87

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). Developing Cyber Peacekeeping: Observation, Monitoring and Reporting. *arXiv preprint arXiv:1806.02608*.

European Projects

CockpitCI
ATENA
CONCORDIA
FLOURISH



Greece – Competent Authorities

Ministry of Digital Policy, Telecommunications and Media
Directorate Cyber Security

EYP- National Intelligence Service
National CERT

Police
Cyber Crime Division

ADAE - Authority for Communication Security and Privacy

Data Protection Authority (DPA)

Ministry of National Defence (MOD)
Hellenic National Defence General Staff

Telecommunications & Post Commission (EETT)

Cyber Crime Division

Cyberkid.gr, app. Cyberkid

Cyberalert.gr

Feelsafe, app. Feelsafe

National Cyber Security Authority of Greece

- Establishment of a national strategy for the security of network and information systems

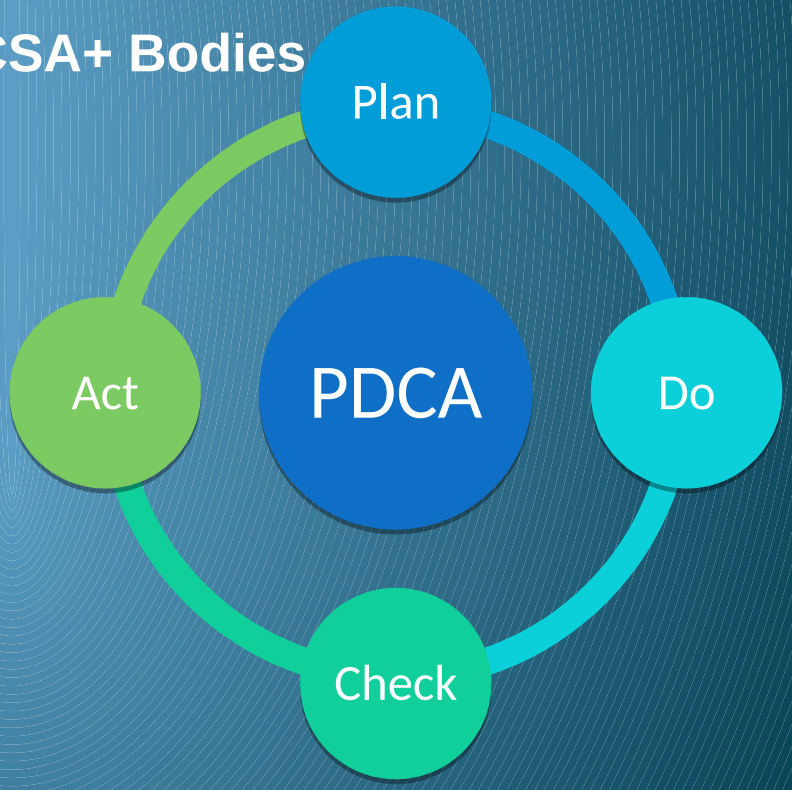
- Representation in the Cooperation Group (NIS)
- Security measures, rules on penalties (NIS)
- List of Operators of Essential Services (NIS)

- Participation in the OSCE
- European Cyber Education, Training, Exercise and Evaluation (ETEE) Platform
- Cooperation with ENISA
- Organization of conferences

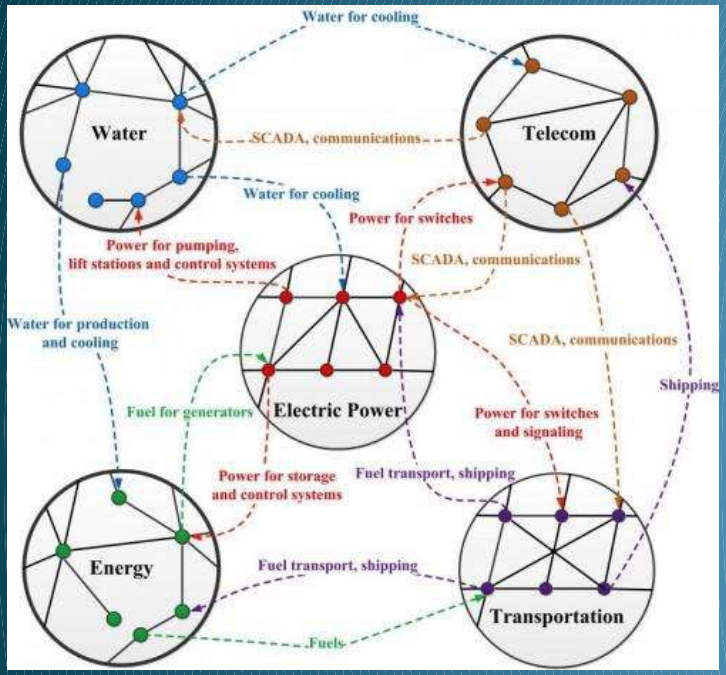
- General overview – IT inventory, security inventory
- Reveal interdependencies, similar configurations and thus vulnerabilities, lack of security measures, creation of a network of Security officers

Lifecycle of Cyber Security Strategy

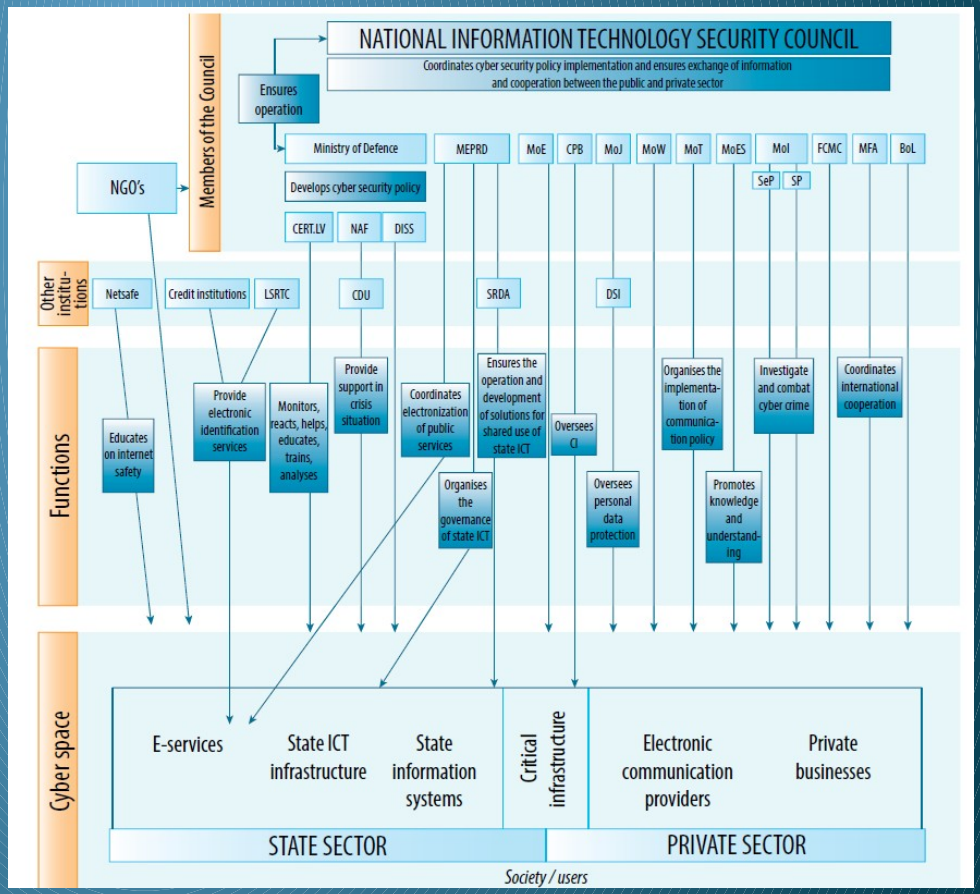
1. Design ⊟ NCSA with Working Groups
2. Implementation ⊟ Bodies
3. Evaluation ⊟ Under the supervision of the NCSA
    1. Internal (Self-Assessment)
    2. External (Outsourcing)
4. Correction / Redefining ⊟ NCSA+ Bodies



Multi-sector interdependencies of critical infrastructure networks



Interdisciplinary collaboration is the key for understanding how to assess the SECURITY AND RELIABILITY of infrastructure and how to make it more resilient



Necessity to create an effective cyber security governance model

Any question ?