Convegno tecnico

Giornata Mondiale della Sicurezza:
Sicurezza Informatica e Pubblica Amministrazione

Cyber security: esperienze e strategie europee

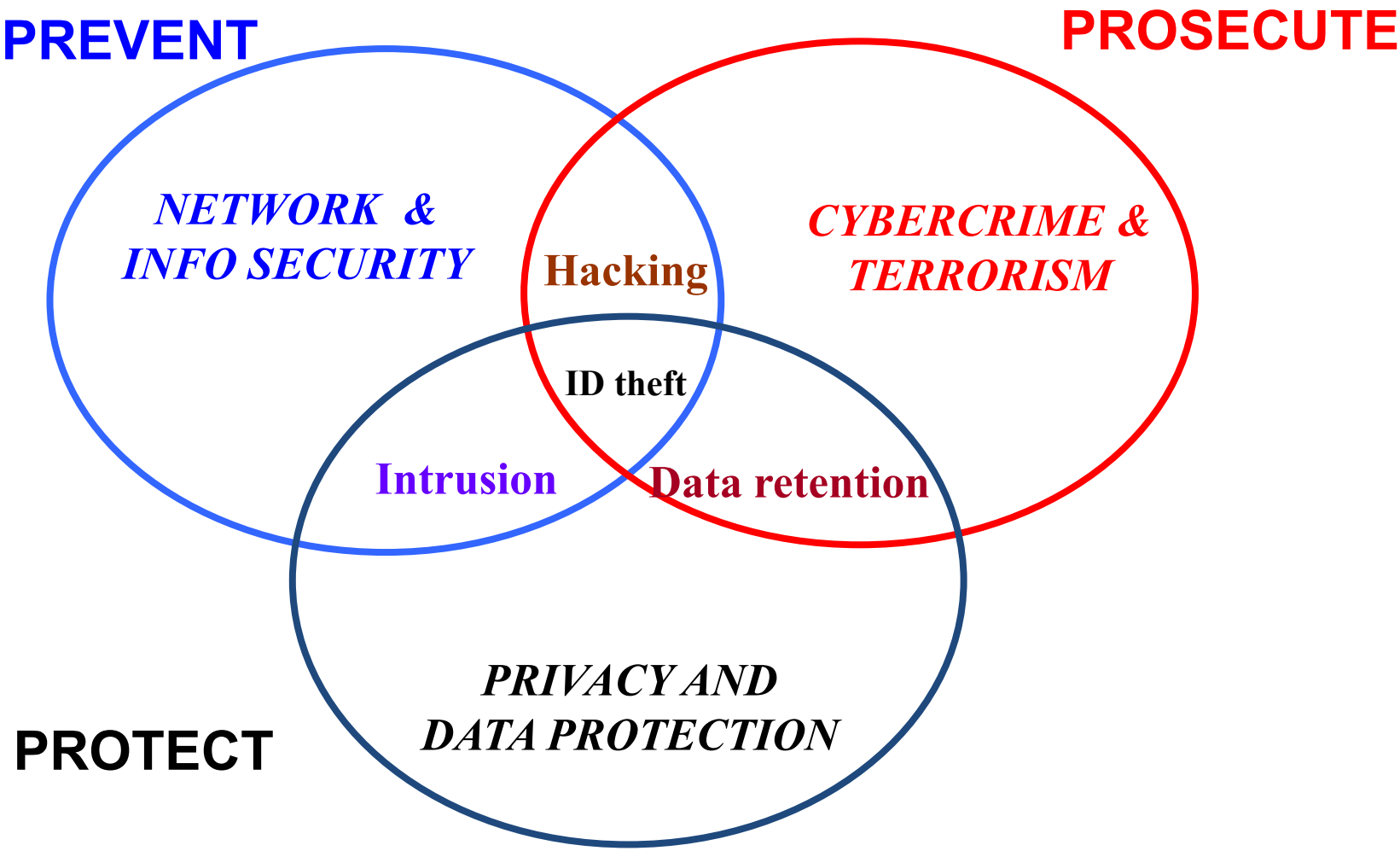
Prof. Ing. Claudio Cilli

28 Aprile 2016

Cyber security challenges are global

- Internet has become the nervous system of our Society
  → **economic and societal dimension**
- Liberalisation, deregulation and convergence
  → **complexity / multiplicity of players**
- Information infrastructures are privately owned and operated
  → **accountability vs. control**
- Ensuring the stability of society and economy is governments' primary responsibility
  → **governance**
- Information infrastructures go well beyond national borders
  → **globalisation**
- The level of security in any country depends on the level of security put in place outside the national borders
  → **sovereignty**
- All Governments face very similar issues and challenges
  → **scale**
- Private sector is calling for legal certainty & harmonised rules
  → **market dimension**

Three angles for actions



How EU is structured around cyber

- EU is organized and managed in a way to **preserve each member's autonomy and jurisdiction**. Therefore – with the exception of some topics covered by the UE Foundation Charter – its role is only as advisor and coordinator, if requested
- National security, and therefore, cyber security are **NOT within the EU constitution**
- Each Country has their military force and line of command
- Every member of the EU Commission is **responsible** for one or more services
- **Security is splitted into some sectors** (e.g.: intelligence, homeland security, migration flows, passport unification, etc., coordination, ENISA, companies security, security of communication, transportation security, energy security, home security and cybercrime)

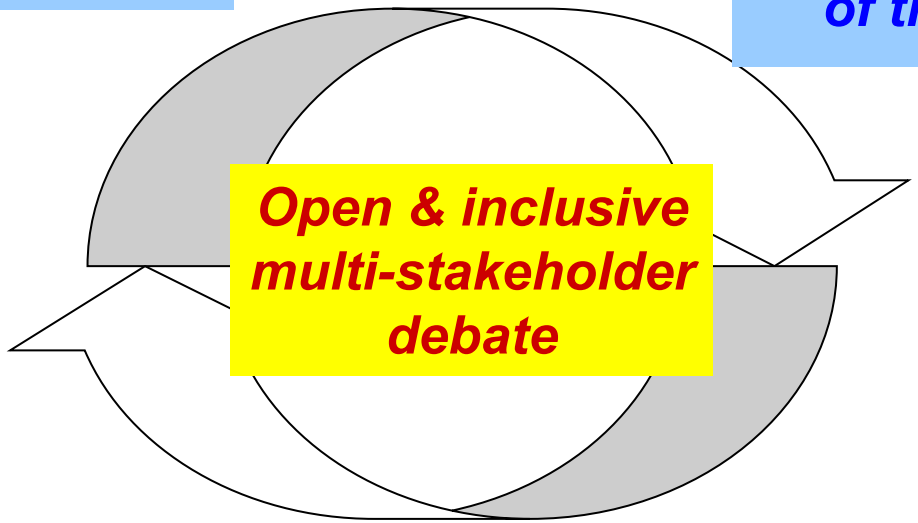
How EU is structured around cyber

- The EU Commission's role is limited to **decide policies** in the field of crime fight
- The EU **policy is to safeguard each Country autonomy above all**. Therefore, the role of the EU Commission regarding cyber security is to help prevention and to involve economic actors (i.e. private companies)
- Within the EU Commission, cyber defense is a **military agency** whose role is to provide advisory and consultancy services to the Commission itself, in order to fund a specific program (FP7 – Framework Program, Security Program which includes cyber security)

EU Policy mechanisms

DIALOGUE
structured and multi-stakeholder

PARTNERSHIP
greater awareness & better understanding of the challenges



EMPOWERMENT
commitment to responsibilities of all actors involved

Cyber security: the EU Policy

- Focus on **prevention, resilience and preparedness** (complementary to fighting **cyber crime**)
- Take into account the **civilian** & **economic stakeholders**' role and capability (role of private sector & the **governance challenge**)
- Make **security and resilience** the **frontline of defence**
- Adopt an **all-hazards approach**
- Develop a **risk management** culture in the EU
- Focus on the role socio-economic **incentives**
- Promote **openness, diversity, interoperability, usability, competition** as inherent security safeguards
- Boost a global **collaborative policy** and **operational cooperation** across the EU, in particular on CIIP

European Strategy for Internet Security
Main Initiatives at EU level so far

- Establishment of **ENISA** - Regulation (EC) No 460/2004
- The Strategy for a **Secure Information Society** (COM(2006)251)
- The Commission Communication on **Critical Information Infrastructure protection** (COM(2009) 149) proposing an Action Plan
- Trust and Security chapter of the **Digital Agenda** for Europe (COM(2010)245)
- The proposal to **modernise ENISA** (COM(2010)521)
- The second Commission Communication on CIIP of March 2011 'Achievements and next steps: **towards global cyber-security**' (COM(2011) 163)
- The revised **Regulatory Framework for electronic communications** – new security provisions including security breaches notifications (Art. 13 a and b)

Internet Security - What is the problem?
An evolving scenario – Threats and risks

Steady growth in number, scope, sophistication of attacks

2007 2008 2009 2010 2011 2012 2013 2014 2015 2016

Estonia

Lithuania

Georgia

Cables cuts in the Mediterranean

Stuxnet

Emission Trading System (EU ETS)

French Government

EC and EEAS

Sony

DigiNotar

…?

10% probability of a major CII (Critical Information Infrastructure) breakdown in the next 10 years – Potential global economic cost of over $250B (Source WEF)

Internet Security - What is the problem?
Economic cost of attacks

A few key examples…

SONY

$175M

EU ETS
€30M

Cybercrime in the UK
£27B/year

Global cybercrime: $388B/year

- Major attack against the EU would cause disruption to:
- Electricity grids
- Critical Information Infrastructures
- Financial services and markets
- Communications networks and infrastructures
- The Single market

E.g. The macroeconomic costs of a major disruption to Switzerland are estimated at 1.2% of GDP (Gross Domestic Product)

European Strategy for Internet Security
The need for further EU action

- Growing **dependence** of our economy and society on the Internet
- Constantly growing **threat** landscape
  - → Need to protect the Internet in order to ensure the
  - proper functioning of the Single Market
- Insufficient preparedness and fragmented approach at EU level
  - → Need for **stronger political commitment** to Internet
  - security efforts
  - → Need for a **strategic** and **comprehensive** approach
- Cross-border implications of security threats
  - → Need for a **EU-wide** and **International cooperation**
- Current measures (under CIIP, DAE [Digital Agenda for Europe]) to be completed by 2012
  - → Need to develop a vision for the years **beyond 2012**

EU Cybersecurity plan to protect open internet and online freedom and opportunity

- The European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, has published a cybersecurity strategy alongside a Commission proposed **directive on Network and Information Security (NIS).**
- The cybersecurity strategy – "**An Open, Safe and Secure Cyberspace**" - represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. This is to further European values of freedom and democracy and ensure the digital economy can safely grow
- Specific actions are aimed at enhancing cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber-security policy and cyber defence

EU Cybersecurity plan to protect open internet and online freedom and opportunity

- The strategy articulates the EU's vision of cyber-security in terms of **five priorities**:
  - Achieving cyber resilience
  - Drastically reducing cybercrime
  - Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
  - Developing the industrial and technological resources for cyber-security
  - Establishing a coherent international cyberspace policy for the European Union and promoting core EU values
- The EU international cyberspace policy promotes the **respect of EU core values**, defines norms for responsible behaviour, advocates the application of existing international laws in cyberspace, while assisting countries outside the EU with cyber-security capacity-building, and promoting international cooperation in cyber issues.

Elements of the future European Strategy for Internet Security (1/4)

Preliminary ideas for legal measures aiming at ensuring the establishment of:

- **Well-functioning National/Governmental CERTs capabilities**
- **An effective network of National competent bodies and Governmental CERTs at EU level (with the necessary protection of confidentiality)**
- **Well-functioning National/Governmental CERTs capabilities**
- **A "European Forum for Regulators" (towards a model for pan-EU cooperation mechanisms – similarly to what is in place in other sectors)**
- **A European cyber-incident contingency plan**
- **General security breach notification obligation (extending Article 13a FD beyond Telcos/ISPs)**
  - Adoption of risk management framework (identification of risks).
  - Adoption of security measures
  - Supervision by competent bodies (including via audit)
  - Notification mechanisms to competent bodies (possibly via CERT function) ensuring confidentiality
- **Mandatory security audits and authorisation mechanisms where this is already required by applicable law (e.g. banking, energy, etc.)**

Elements of the future European Strategy for Internet Security (2/4)

Preliminary ideas for further measures to improve security in networks and services:

- **Incentives for the private sector to improve security in products and services, e.g. through IT security standards in public procurement**
  - Incentives through the public procurement process (via guidelines and standards)
  - Simulating a public-private partnership to reduce the spread of malware
  - Promotion of transparency and competitiveness in the internal market (benchmarks, trusted data on incidents and vulnerabilities, information to users, compliance with standards, certification and self-certification to develop re-assurance market)
- **Awareness raising measures and activities**
  - Mobilization of Member States and stakeholders towards a EU-wide campaign (for instance, a month for Network and Information Security for all)
  - National/European Cyber-security Competitions to foster development of skills
  - International synchronization and coordination of awareness raising messages and campaigns (US and Japan)
  - Reinforced role of ENISA in promoting standards, good practices and a risk management culture

Elements of the future European Strategy for Internet Security (3/4)

Preliminary ideas for further measures to improve security in networks and services:

- **Making the best use of research and innovation and putting in place a robust industrial policy**
- **Adoption of state-of-the-art technologies & processes - Promote take up**
  - stimulate private and public demand (security to be an integral part of the provision of e-services, mandatory for eGov, pre-commercial procurement)
  - develop standards
  - improve usability
- **Reinforcing and coordinating R&D for present and future security challenges**
  - H2020 LEIT => make the technologies available
  - H2020 IIS => put technology to work
  - Underpin the technical feasibility of the cyber security policy and associated actions
  - Create partnerships in cyber-security

Elements of the future European Strategy for Internet Security (4/4)

Preliminary ideas for further measures to improve security in networks and services:

- **Appropriate measures in the area of cybercrime (in cooperation with DG HOME)**
- **Putting the EU in the lead of international discussions on Internet security matters**
  - Promotion and engagement in multilateral cooperation
  - Leveraging EU-US activities towards broader International
  - participation
    - Fighting Botnets
    - Cyber-security of Industrial Control Systems and Smart grids
  - Promotion of EU interests in global Internet security
    - Multi-stakeholder governance
    - Market access
    - European principles and guidelines for Internet resilience and stability
    - COMPACT for the Internet

Governance framework
Roles, responsibilities and structures

- **Main actors - roles and responsibilities**
  - Commission level (&EEAS)
    - Inter-service Group on Cyber-security and Cyber-crime
  - European Commission vis-à-vis other EU institutions (EP, Council, EDPS, CTC, etc.)
    - Interfaces and synergies with other activities, i.e. cybercrime, cyber defence, norms of responsible State behaviour, counter-terrorism, etc.
  - Member States (EFMS, relevant CWGs)
  - Private sector (EP3R)
  - ENISA
  - EU-CERT
  - Other Agencies and bodies
- **Governance structure**
  - EU internal
  - International (bilateral relations and multilateral fora, e.g OECD, UN, G8, etc)
  - Need for a new platform?

Technical guidelines on reporting security breaches by ENISA

e-Communications security and resilience
ENISA good practices

- Technical Guidelines on Reporting Incidents – Guidance on incident reporting scheme in Article 13a
- Shortlisting network and information security standards and good practices
- Technical for Minimum Security Measures – Guidance on the security measures in Article 13a
- Implementation of Article 4 - Recommendations for the technical implementation of the Article 4 of the ePrivacy Directive
- Inter-X: Resilience of the Internet Interconnection Ecosystem
- …

Policy developments on fighting botnets Background

- **Member States**: DK, DE, NL, SE, IT
- **Outside EU**: Australia, Japan, South Korean
- **EU level**: i) 2011 ENISA study & policy statement on botnets; ii) botnet is a priority of EP3R-WG3
- **International level**: i) EU-US WG on cyber-security and cyber-crime; ii) OECD's study on the role of ISPs in botnet mitigation

EP3R-WG3 activity on fighting botnets

- Pursuing at EU level **national anti-botnet efforts**
- Putting together existing operational and concrete **good practices** (including Awareness Raising)
- **Service to report and receive** automated, standardised details about botnet infected end-user systems
- Provide **legal & technical support** to the victims of DDoS / botnets
- **Drive-by Infection Website-check for SMEs**
- **Overcome legal constraints to exchange information** to fight botnets across borders

EU-US WG on Cybersecurity and Cybercrime ESG on PPP

- **Fighting botnets - EU-US experiences**

- Tracking down communication channels between masters and bots
- Removing botnets by supporting end users
- Cleaning infected websites
- Mitigating the impact of cyber attacks based on botnets

- **→Towards and International cooperation framework**

Fighting botnets
ENISA good practices

- Botnets: Detection, Measurement, Disinfection & Defence
- Botnets: 10 Tough Questions
- Legal analysis and recommendations (in preparation)

Policy activity

Security and Resilience of communication networks and information systems for the Smart Grid

EU Expert Group: objectives

- Identify European **priority areas** for which actions should be undertaken to address the security and resilience of communication networks and information systems for Smart Grids.

- **Define recommendations** on how to progress on each priority area at European level.

- **Identify the critical elements of to be addressed** (e.g. smart appliances, smart metering, smart distribution, smart (local) generation, smart transmission, etc).

EU Expert Group on ICT security and resilience for smart grids - Program of Work

2.1. Risks, threats and vulnerabilities

WP 1.1. Identify and categorize all relevant Smart Grid assets

WP 1.2. Develop an attack / threat taxonomy for relevant assets

WP 1.3. Develop a countermeasure taxonomy for relevant assets

WP 1.4. Develop a high-level security risk assessment methodology for relevant assets

2.2. Requirements and technology

WP 2.1. Security Requirements

WP 2.2. Extend Smart Grid requirements to include effective security measures

WP 2.3. Research Smart Grid communication protocols and infrastructures to incorporate data security measures

WP 2.4. (Public) procurement

2.3. Information and knowledge sharing

WP 3.1. Develop a cross-border alliance between Member States and relevant competent bodies and

2.4. Awareness, Education & Training

WP 4.1. High level Conference for strategic leaders

WP 4.2. Propose initiatives to increase stakeholder awareness on data security

WP 4.3. Skilled personnel on cyber security in energy industry

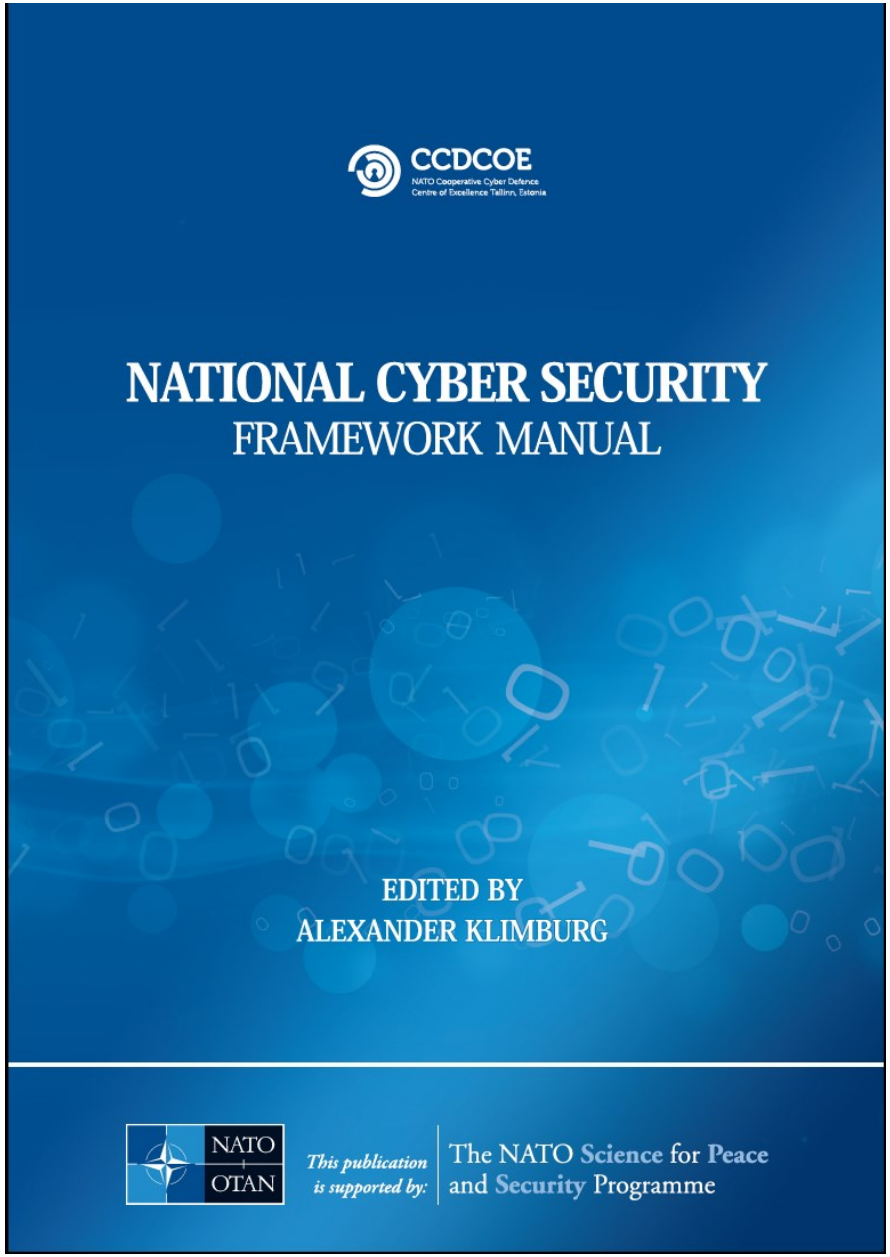
EU-US WG on Cybersecurity and Cybercrime ESG on PPP

- **Cyber security of ICS and smart grids - EU-US experiences**
  - Information sharing
  - Guidelines for vendors
  - Sharing vulnerabilities to coordinate response to incidents
  - Training and awareness raising (C-level)
  - R&D

- **→Foster International cooperation – International Conference**

Role of NATO

- Not all EU countries are NATO members. This creates security matters. Therefore any attempt to strictly co-operate with NATO beyond advisory and consultancy is prevented
- NATO has established a Cyber Defense Management Authority. After the announcement (2009) some cooperation started

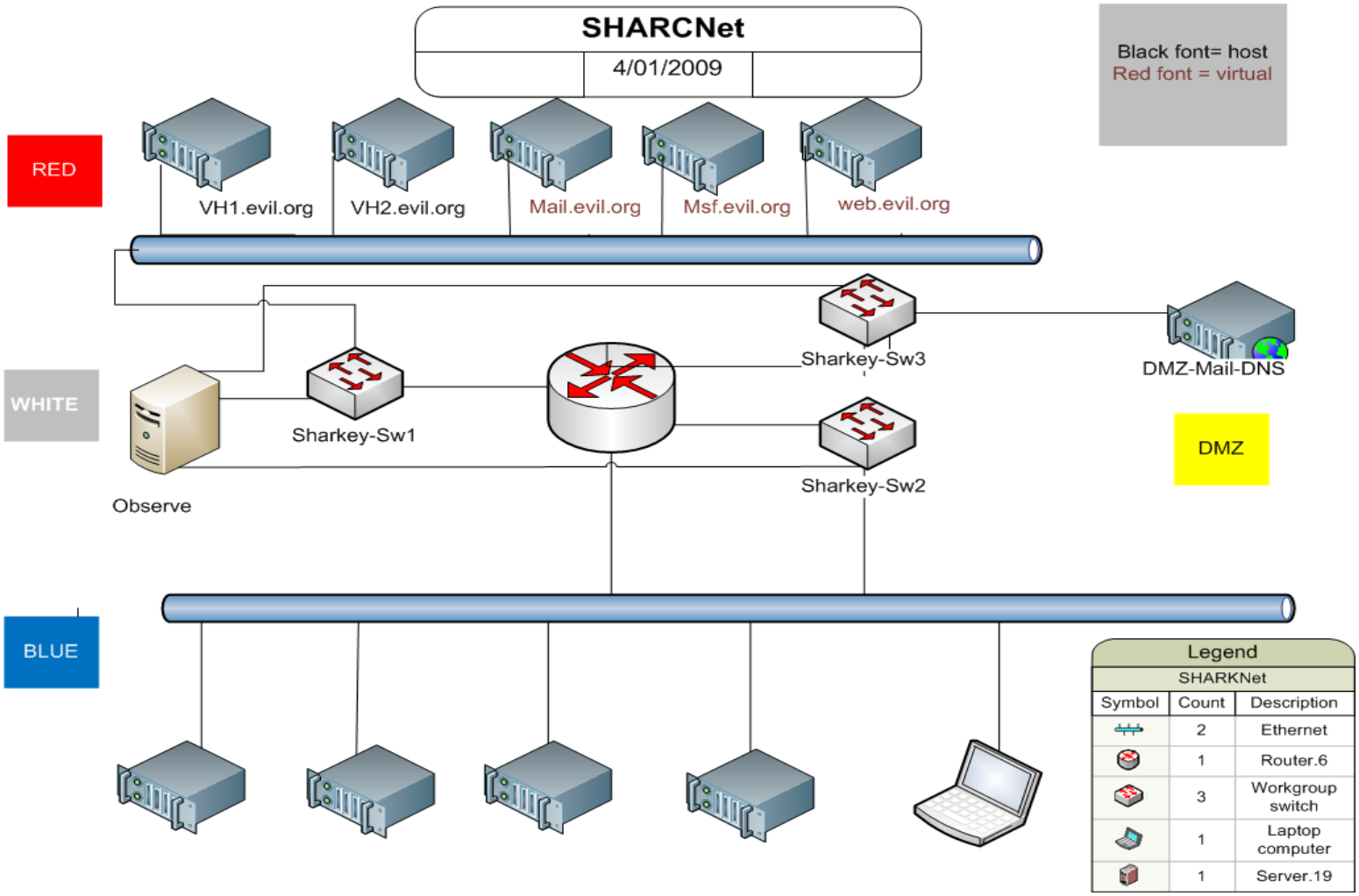

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia
NATIONAL CYBER SECURITY
FRAMEWORK MANUAL
EDITED BY
ALEXANDER KLIMBURG
NATO OTAN
This publication is supported by:
The NATO Science for Peace and Security Programme

The Structured Holistic Attack Research Computer Network (SHARCNet)

- Overview
  - SHARCNet allows for the Research, Development, Testing, and Evaluation of the most state of the art technologies for Cyber Warfare & Security.
  - Structure
    - Red Cell fully demonstrates CNA/CNE vectors
    - Blue Cell fully demonstrates CND Defense-in-Depth Strategies and contains:
      - An Armored or Hardened Segment (Citadel)
      - A Vulnerable Segment (Victim)
    - White Cell provides Qualitative and Quantitative Cyber Security Analysis, Digital Forensics, & Autopsy.

Cyber Warfare Modeling & Simulation

Cyber Range System Architecture



Computer Network Attack (CNA)

- **SHARCNet RED Cell Operations**
  - Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves.
  - The Four D's of CNA
    - **Degrade**
      - Data Corruption
    - **Disrupt**
      - Malicious Code, Weapons of Mass Disruption (WMD)
    - **Deny**
      - Distributed Denial of Service (DDOS), BotNets
    - **Destroy**
      - Permanent Denial of Service (PDOS), Non-Kinetic / Kinetic Response

Network Attack Modeling

Computer Network Exploitation (CNE)

- **Enhanced RED Cell Operations**
  - Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.
    - Cyber **I**ntelligence Compilation
    - Cyber **S**urveillance
    - Cyber **R**econnaissance
    - Cyber **C**ounterintelligence

Network Exploitation Modeling

Computer Network Defense (CND)

- **SHARCNet BLUE Cell Operations**
  - Includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks.
  - The Defense-in-Depth approach is to defend a system against any particular attack using several, varying methods. It is a layering tactic which was conceived as a comprehensive approach to information and electronic security.
  - Substructure includes:
    - A Citadel Segment (Armored – Dynamic Defense)
    - A Victim Segment (Vulnerable)

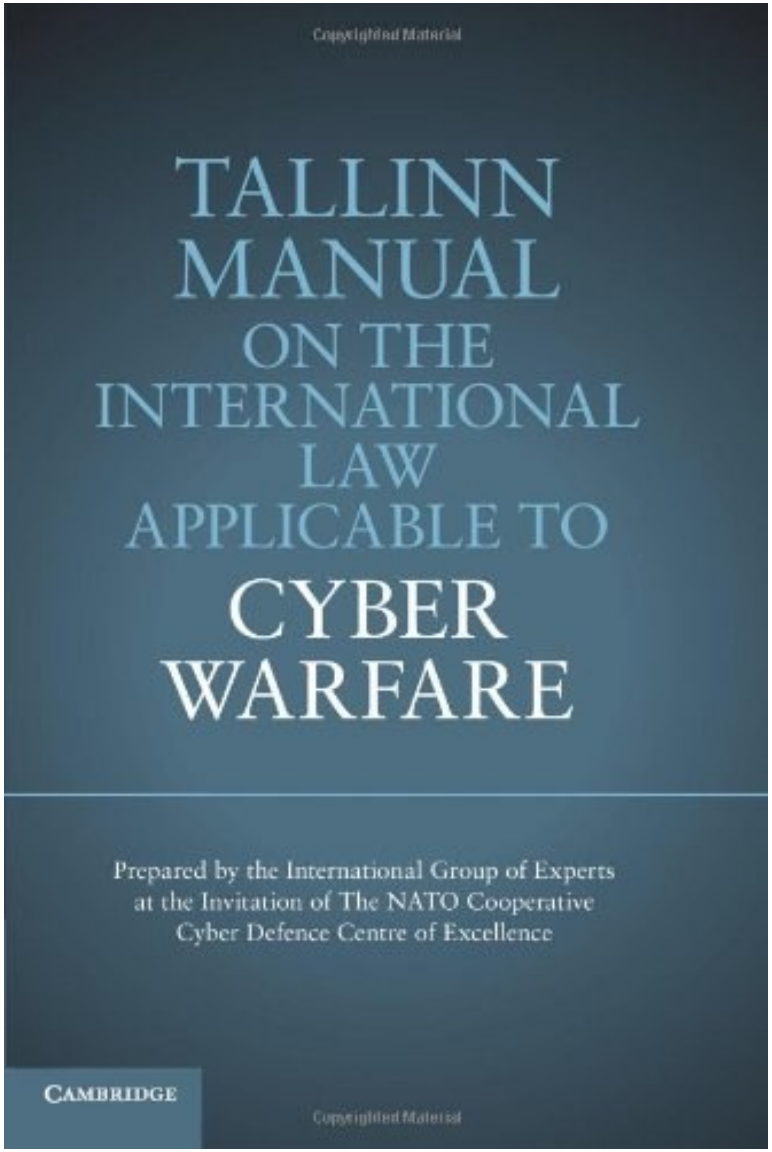
Network Defense-in-Depth Modeling

35

CNO Monitoring & Collection

- **SHARCNet** WHITE Cell Operations
  - Neutral Objectives
    - Observe
    - Monitor
    - Collect
    - Analyze (Digital Forensics & Autopsy)
    - HoneyNet / HoneyPot Analysis

Real-time Research & Analysis


Copyrighted Material
TALLINN MANUAL
ON THE INTERNATIONAL LAW APPLICABLE TO
CYBER WARFARE
Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence
CAMBRIDGE
Copyrighted Material

Thanks for your attention!