10ο Συνέδριο Security Project 2023

NTT DATA

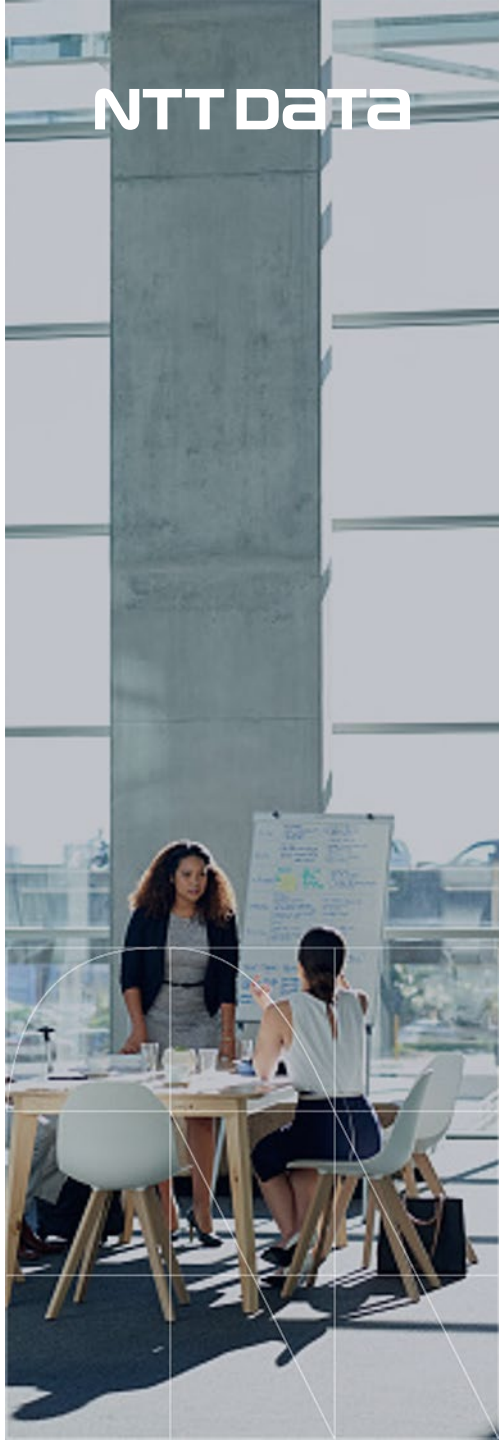
Οι υβριδικές απειλές ασφάλειας και ο ενεργητικός τρόπος αντιμετώπισης τους

Presented by: Notis Iliopoulos, Cyber Security Senior Manager, MSc InfoSec, MSc MBIT, CISA, CISM

Date: 30/03/2023

Agenda

1. Hybrid security threats
2. Active defense @ the corporate environment
3. Security risk management, the holistic approach
4. How to



Hybrid threats

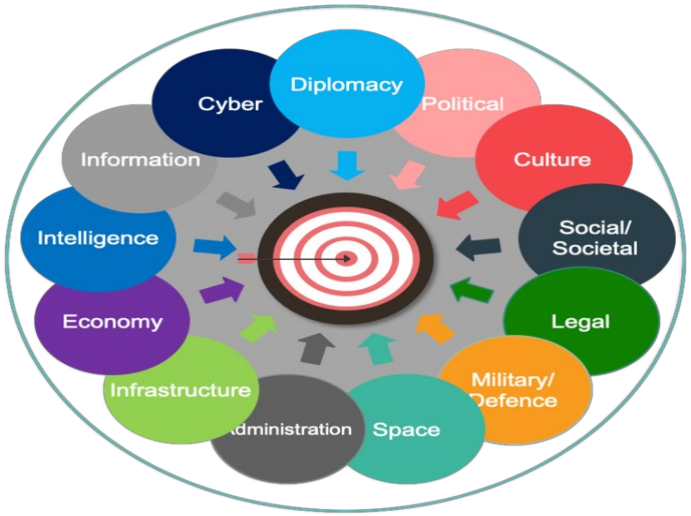


Figure 4. Domains of the conceptual model[17]

Mixture of coercive & subversive activity, conventional and un-conventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare

The EU's 'Joint Framework on Countering Hybrid Threats'

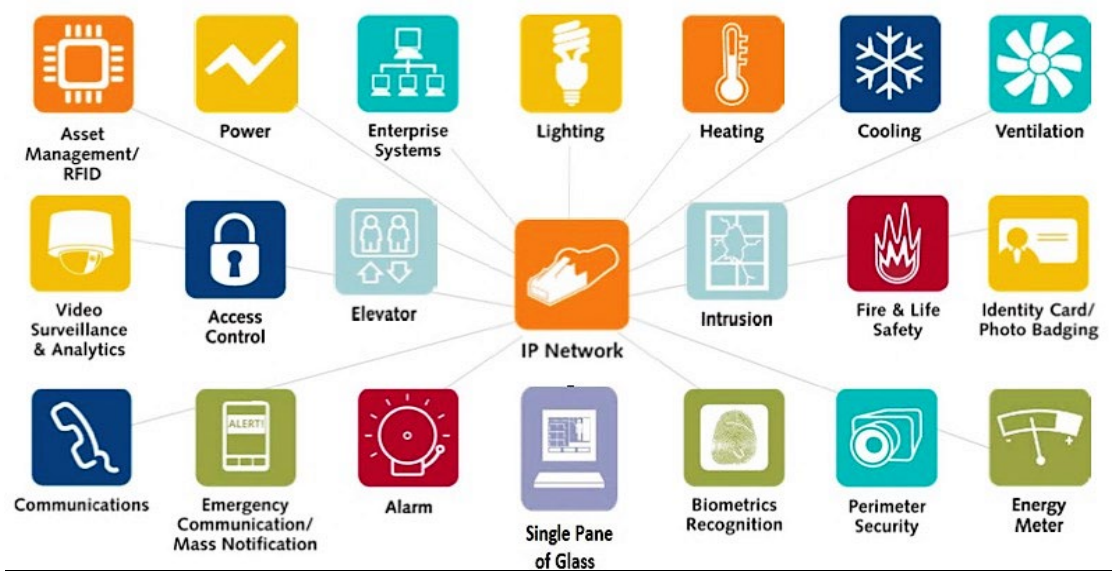
Hybrid threats can range from cyberattacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social divisions

The EU External Action Service (EEAS)

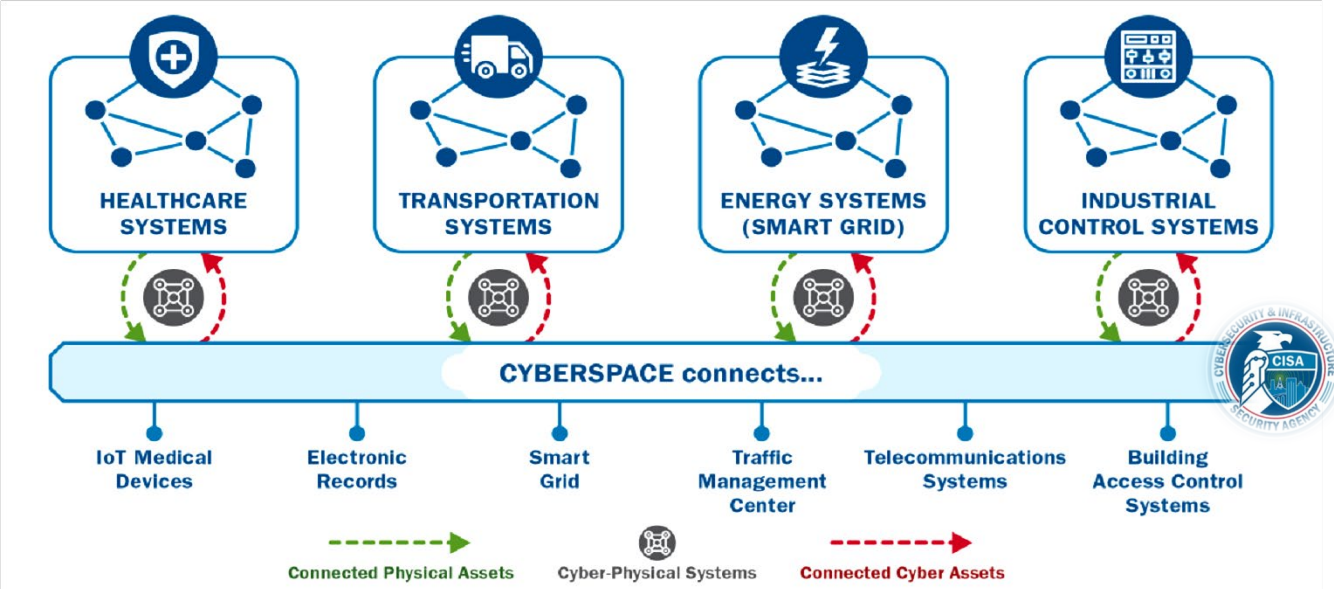
Hybrid threat activity targets a state in multiple domains by applying combinations of tools. Each tool targets one or multiple domains, or the interface between them, by creating or exploiting a vulnerability or taking advantage of an opportunity

EU Hybrid CoE

Hybrid security threat scenarios



- An attacker breaks into a server room and installs rogue devices that capture confidential data
- The internet drop line is accessible from outside of the building, allowing an attacker to intercept data or cut the line completely.
- An inside actor looks over the shoulder of a system engineer
- An attacker pretends to be an employee



- Put surveillance systems out of service or take control of them
- Access and damage elevator control systems, gates, or the entire power system
- Take control of connected devices such as cameras to retrieve sensitive data or to use as an internal attack vector

Security convergence

Integrated security across the entire organization, connects a wide range of security processes

Centralized visibility & incident response

Effectiveness & economies of scale, adoption of controls and unification of operations

Convergence of the, CSO, and CISO roles

Incident handing & threat operations centers

- **Handling** any type of critical security incidents
- The typical steps to mitigate the impact of any of the major **security incidents** are very much the same
- A physical intrusion might have an **impact** on safety and security, not just on people but on systems
- Many companies are creating **converged response teams** where they can handle all security events

Incident handing & threat operations centers

- **Converged centers** that handle all security events and respond to all security incidents, crisis management coordination
- **Continuously monitors** Threat Intelligence, Analytics, Threat Detection, Incident Response, Threat Hunting, CCTV Monitoring, Asset and Person Tracking, Intelligence Analysis
- **Active threat management** that also includes, controls assessment, read teaming & crisis management exercises, continuous update of the threat profile and the response playbooks
- **Active detection** of security vulnerabilities related to any security discipline

Incident handing & threat operations centers

- **Banking organization** - Have maintained mixed teams for years, with a particular focus on incorporating fraud-detection functions with other cybersecurity disciplines
- **Health-care device maker** - Added 24/7 monitoring of physical and cyber issues that might affect business systems, medical devices and healthcare information
- **Health care & insurance giant** - Have structured cybersecurity and physical security organizations to report to a single CSO, the companies confirmed

Convergence in roles & structures

The CxO-level role that leads this effort will be responsible for security risk, business continuity, physical, and information security

Integration of teams that manage physical and Digital/Information security, as well as crisis response, into a single center

Virtual collaboration among these teams is the first step

Physical, digital and crisis groups could be increasingly housed together in a SoC

Keeping these teams in one place helps support testing and monitoring for Digital intrusions as well as physical break-ins

Physical and IT security roles will still be required, but with more communication among those roles and much more integration of solutions and processes

How to align Corporate Security disciplines

Include physical and digital security, regulatory compliance, info security, crisis management and business continuity, loss prevention, brand protection, travel risk, supply chain security and workplace violence prevention

How to align Corporate Security disciplines

Challenge 1

Lack of uniform, consistent standards

Challenge 2

Historical biases & traditional silos

Challenge 3

Update/build new skills & bridge the skill & language gap

Challenge 4

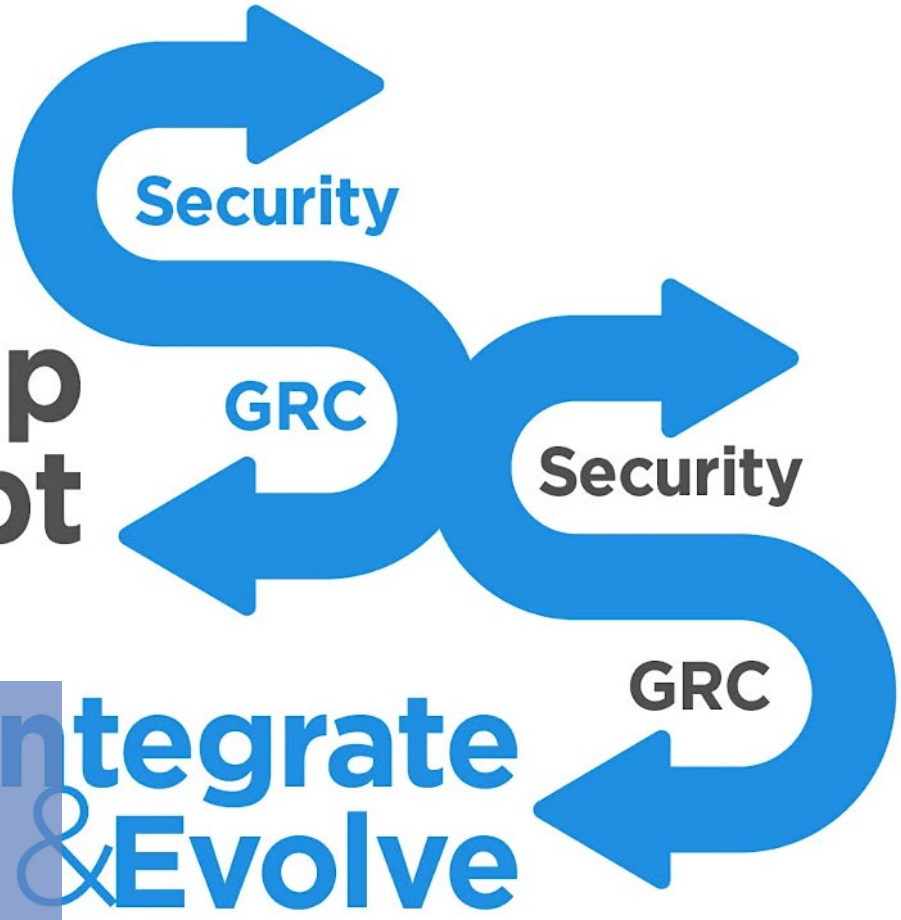
Assignment of roles & responsibilities

Challenge 5

Convergence in Security Solutions

- Develop and Adopt a Security Governance & Compliance framework
- Adopt a holistic Security Risk Management methodology

- Unify security operations
- Establish metrics & common reporting
- Continuous reporting & enhancement of adoption



[1] Notis Iliopoulos, Proposed approach for the effective implementation of Converged Security Governance & Risk Management in the corporate environment, 2021

The changing face of corporate security

Information Assurance

- Confidentiality
- Integrity

Continuity of operations & safety

- Availability
- Safety

- Authenticity
- Confidentiality

Security Governance & Risk Management

Unified Security Operations

Keep in touch.

Notis Iliopoulos

Panagiotis.iliopoulos@nttdata.com