



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



NATIONAL CYBER SECURITY CENTRE

TLP:AMBER

Overview of National Cyber Security



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



NCDS Working Group

28th September 2023

NCDS Working Group 28th September 2023



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

A faint, light blue network diagram consisting of numerous circular nodes connected by thin lines, forming a complex web-like structure that serves as a background for the title text.

OVERVIEW OF THE NATIONAL CYBER SECURITY CENTRE

NCDS Working Group 28th September 2023



Rialtas na hÉireann Government of Ireland



**An Roinn Comhshaoil,
Aeráide agus Cumarsáide**
Department of the Environment,
Climate and Communications



**An Roinn Comhshaoil,
Aeráide agus Cumarsáide**
Department of the Environment,
Climate and Communications



Mission



Leading Ireland's Response to Cyber Risk



What we do



**INCIDENT DETECTION
& RESPONSE**



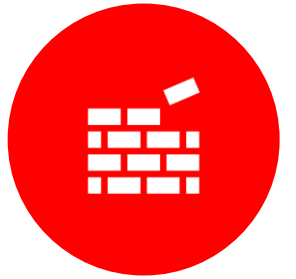
**RISK ANALYSIS &
SITUATIONAL
AWARENESS**



ENGAGEMENT



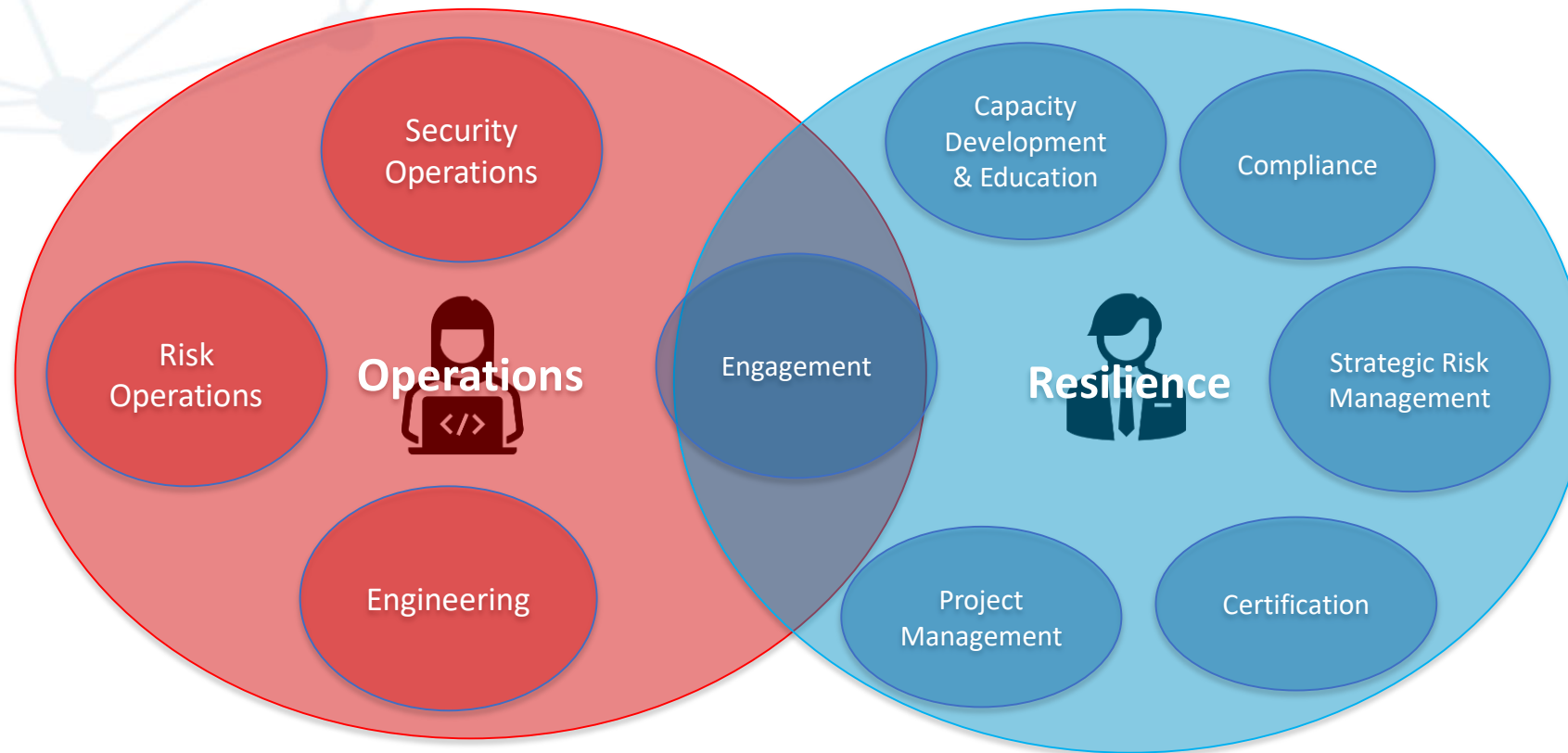
CYBER RESILIENCE



CAPACITY BUILDING



NCSC Teams



Operations

- Incident Triage
- Incident Response
- Malware Analysis
- Cyber Exercises

Security
Operations



- Threat Intelligence
- Vulnerability Management
- Active Cyber Defence

Risk
Operations



- IT Admin
- Programming & Development
- Sensor Program

Engineering



Resilience

- Government
- CNI
- Business
- International
- Guidance

Engagement

- EU Cybersecurity Act
- Cyber Security Standards
- Certification

Certification

- NIS Competent Authority
- OES Self-Assessments
- Audits

Compliance

- National Cybersecurity Competence Centre
- Research Funding
- Education

Capacity Building

- Plans & Budgets
- Project Tracking
- Governance
- Training

Project Management

- Strategic Risk
- NIS2...

Others...





INTERNATIONAL PARTNERS



 National Cyber Security Centre
a part of GCHQ

NATIONAL PARTNERS



Industry



MANDIANT



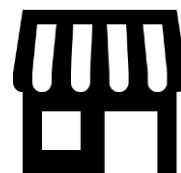
Academia



CONSTITUENTS



Digital Service Providers



Business



Citizens



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

A faint, stylized network diagram is centered in the background. It consists of numerous circular nodes connected by thin lines, forming a complex web that suggests interconnectedness and data flow.

Hybrid and cyber threats

NCDS Working Group 28th September 2023

What is Cyberspace

Recognised by NATO as a domain of operations

Cyberspace is NOT the internet – 3 layers



3. Cyber-persona layer

2. Logical layer

1. Physical layer



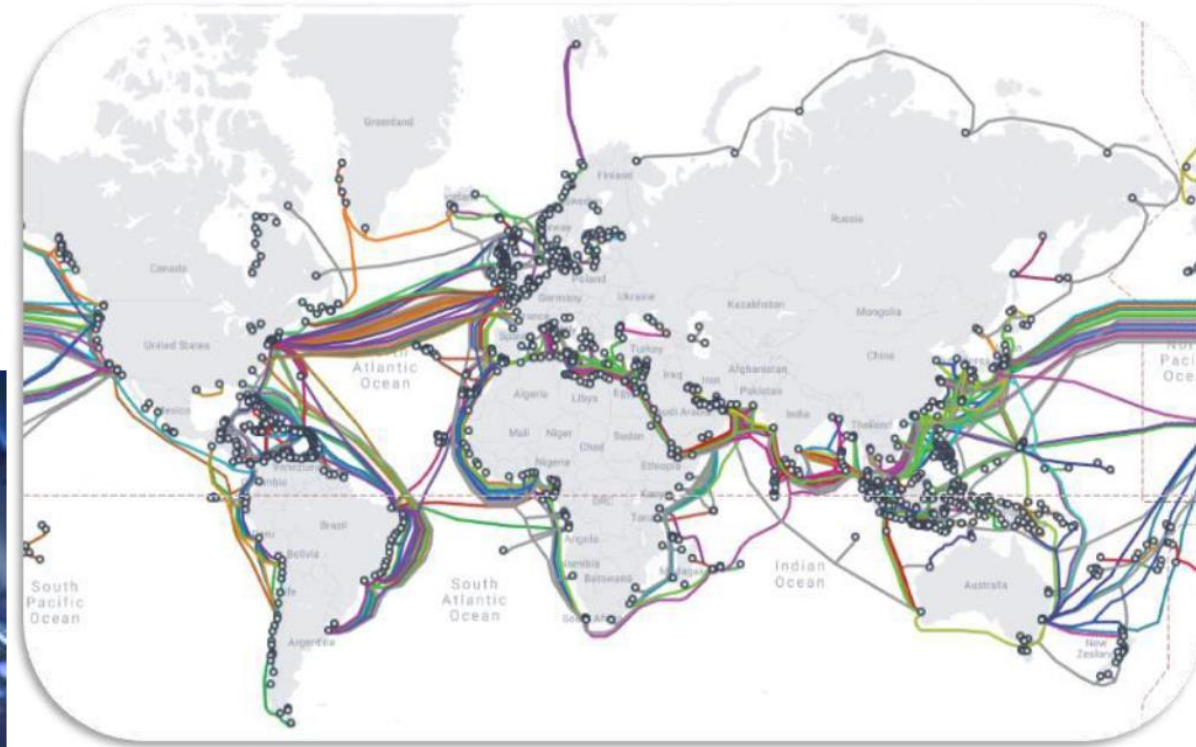
What is Cyberspace

Physical Layer

- Signals
- Systems
- Environment
- Living world
- infrastructure



Physical Layer

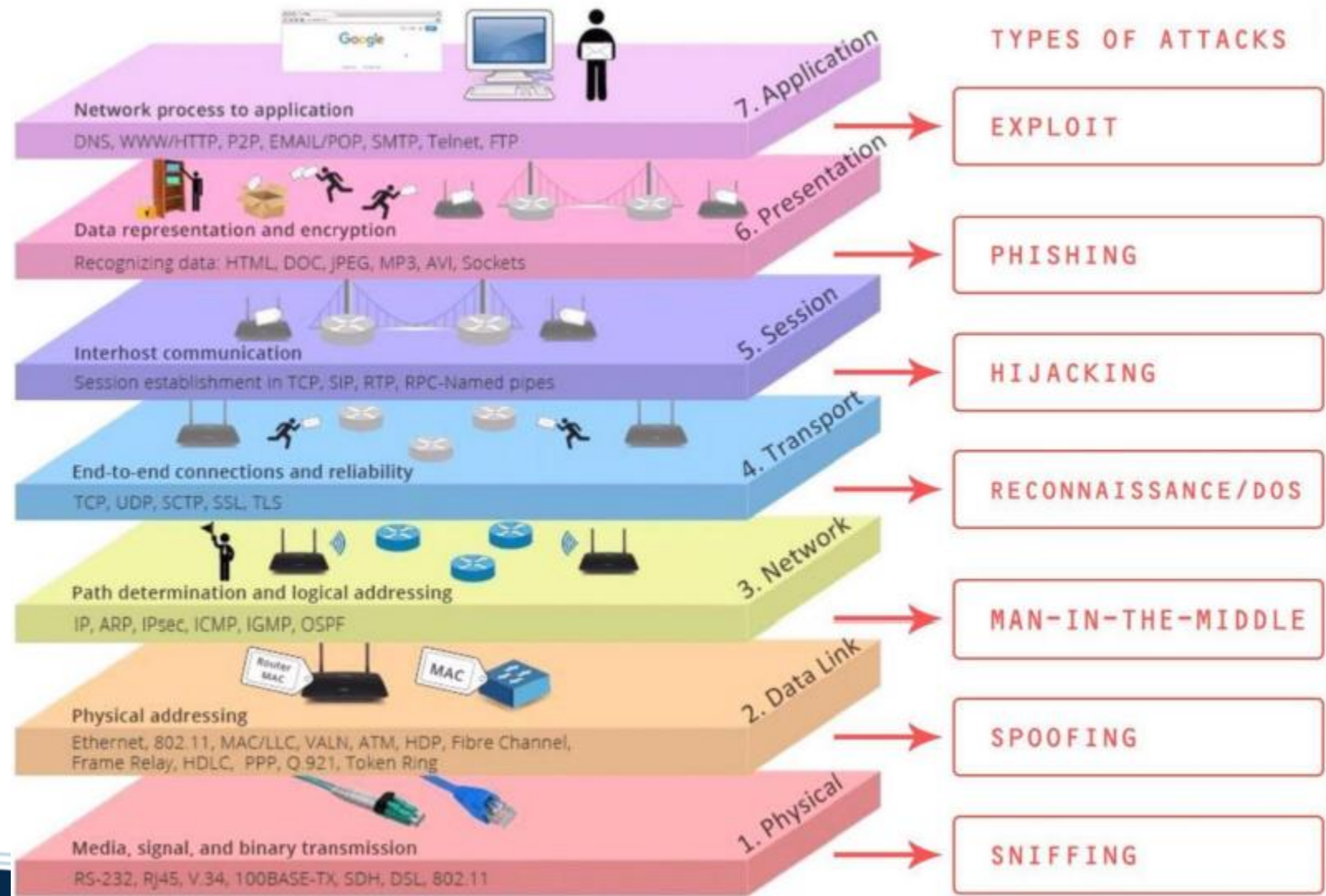


What is Cyberspace

Logical Layer

Logical layer

- Data
- Algorithms
- services

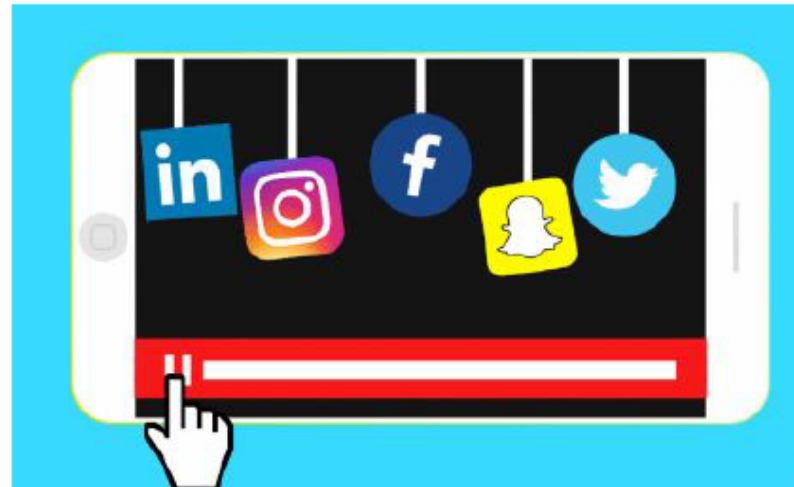


What is Cyberspace

Persona layer

- Human and cognitive aspects
- Information
- Knowledge
- Will
- An individual can have multiple personas
- Multiple different users may share a single persona

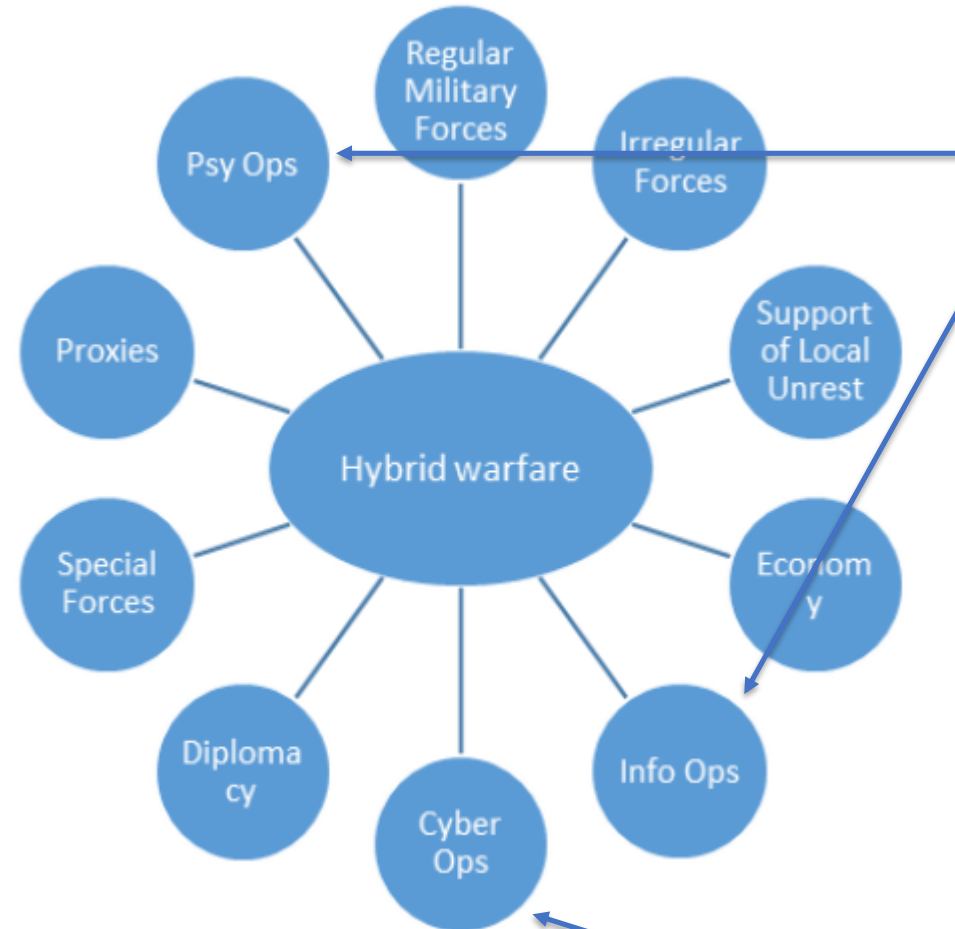
Persona Layer



Cyber v MDM/FIMI

This slide illustrates how **cyber** and **MDM/FIMI** relates to hybrid conflict

- Cyber enabled – MDM, FIMI
 - through cyber space, cyberspace not target
- Cyber dependent – disrupt CNI
 - long lead in time, use once, but pre-positioning for immediate effect



Information warfare designed to create confusion, uncertainty or doubt in the population

- Don't expect isolated cyber attacks
- Expect persistent cyber effects combined with InfOps, PsyOps, etc

Disrupt critical infrastructure



Cyberspace – threat actors

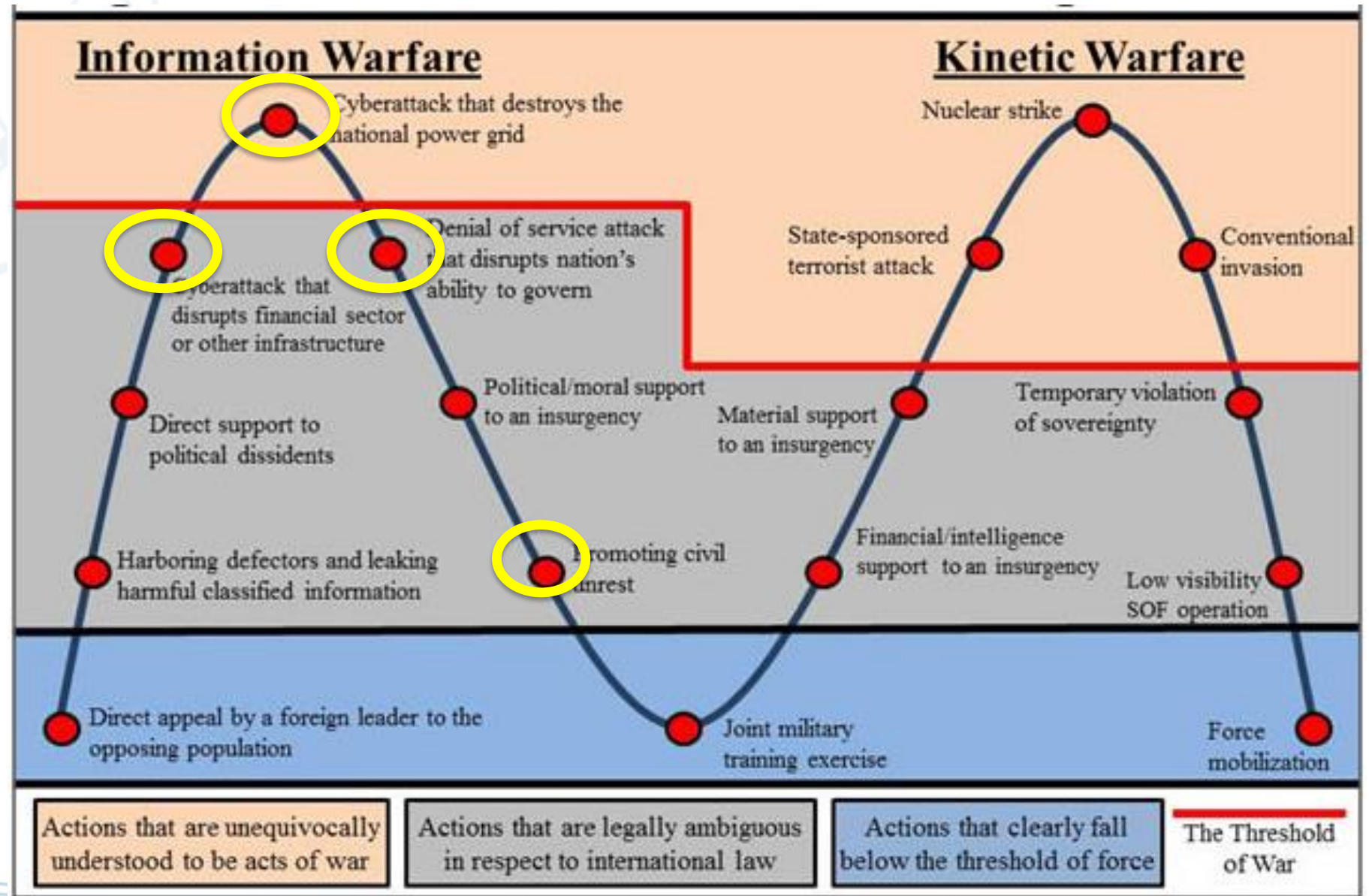


- Authoritarian states can impose themselves on commercial companies and individuals
- Rising cooperation between RU and CH in the fields of cyber and cyber threats
- Rule by law v rule of law



Spectrum of Nation-State Warfare Operations

EU speaks of cyber conflict, not cyber war – grey zone



Characteristics of Hybrid threats

Democratic systems can be weakened by threat actors who target certain systematic vulnerabilities

Hybrid threat is a western concept to describe 21st century challenges


Characterise hybrid threats

- coordinated, synchronised action (target democratic states by a wide range of means)
- conventional and unconventional tactics across multiple domains
- exploit thresholds of detection, attribution and interfaces (grey zone, war & peace, friend enemy, virtual real, internal external etc)
- cognitive warfare – influence decision making, attitudes and behaviours
- overlap between threat actors
- salami tactics





An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

A large, faint network diagram consisting of numerous interconnected nodes and lines, forming a complex web-like structure, is centered in the background of the slide.

C o u n t e r m e a s u r e s

N C D S W o r k i n g G r o u p 2 8 t h S e p t e m b e r 2 0 2 3

Online Operations Kill Chain



NCSC works with platforms to identify threats

Research conducted in Ireland indicates that information provided by platforms is often vague and unreliable.

The DSA makes provision for vetted researchers to access data from major platforms.

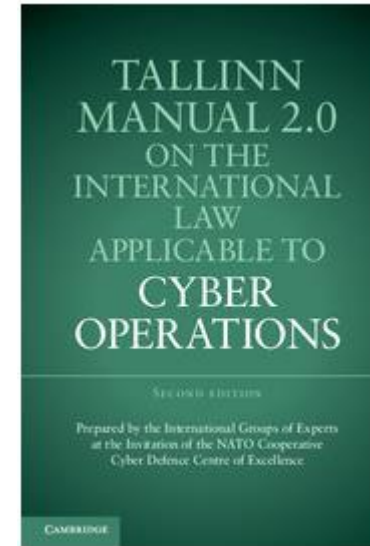


Countering hybrid threats – cyber and MDM/FIMI

- EU speaks of cyber conflict, not cyber war (grey zone)
- Strategic approach required to leverage tools and advance the ability to attribute malicious cyber activities
- Setting norms in international fora (UN) is central to promoting rules based world order
 - UN GGE, OEWG
 - CCDCOE – cyber law toolkit
 - Tallinn manual 2.0 – non binding opinion of experts
 - Irish position paper on “application of international law in cyber space”

International Cyber Law in Practice: Interactive Toolkit

Welcome to the Cyber Law Toolkit, an interactive online resource on international law and cyber operations.



An Roinn Gnóthaí Eachtracha
Department of Foreign Affairs



An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications



Countering hybrid threats – cyber and MDM/FIMI

- EU Cyber Solidarity Act (proposed) - **enhance situational awareness and response**
 - Cybersecurity shield
 - Cyber emergency mechanism (preparedness actions, cyber reserve, mutual assistance)

The NCSC are building enhanced situational awareness capability through tooling and collaboration partnerships

- Toolboxes ➡ **EU Hybrid Threats, Cyber Diplomacy, FIMI**
 - Sanctions and other restrictive measures are thus far the heaviest tools in the boxes
 - **not yet an integrated approach across EU cyber crisis mechanisms and toolboxes**
- NIS2 – resilience, DNS measures





An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

A faint, stylized network diagram consisting of numerous interconnected nodes and lines, resembling a web or a complex system, is centered in the background of the slide.

Security of the Electoral process

NCDS Working Group 28th September 2023

NCSC

NATIONAL CYBER SECURITY CENTRE

Quick Guide: Cyber Security Best Practice for Electoral Candidates



Common Cyber Attacks



Hack and Leak

Hacking of messaging service, social media and e-mail accounts to steal sensitive data which is then leaked publicly to discredit an individual candidate. Sometimes attackers will alter documents or plant false leaks amongst the facts in their release of information.



Defacement

Hacking of social media accounts and candidate websites to deface them or publish damaging disinformation.



Malicious Insider

Leaking of sensitive information by an insider to expose internal communications between members of a group.



A part of the **Department of the Environment, Climate & Communications**



NCSC Cyber Security for Political Parties and Candidates

Cyber security advice to assist political parties and candidates in securing their IT systems.



2 Cyber security risks for political parties and candidates	3
3 Advice to Candidates	5
3.1 Account Security	5
3.2 Device Security	5
3.3 Phishing	6
3.4 Actions On Compromise	7
4 Guidance For IT Administrators And Support Staff	8
4.1 Phishing, Spear Phishing And Whaling Attacks	8
4.2 Malware	9
4.3 Credential Abuse	10
4.4 Operational Security	10
4.5 Denial Of Service (DoS) And Defacements	10
4.6 Incident Response Planning	11
5 Resources	12

In conclusion..

- Don't consider cyber or MDM/FIMI separate from hybrid
- Countering disinformation requires a whole of society approach
- Building resilience is key, proactive v reactive



Questions

?

