Axel Haas

Disclaimer: Personal professional opinion, no official CCOE, NATO nor national position

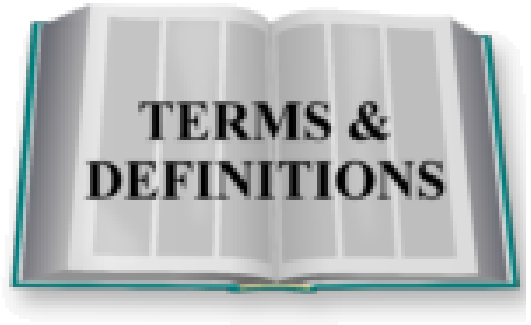
What to Expect

- What threats are we facing in cyberspace? Are Cyber Threats an extension of Hybrid Threats or something completely different?
- How is Resilience in our Allied Nations impacted by the Cyber Domain and Cyber Threats?
- **Which role does NATO play in responding to Hybrid Threats in the Cyber Domain?**
- **How can CIMIC & CMI contribute to enhancing Resilience in the Cyber Domain?**

However: difficult topic, no easy solutions, manage your expectations

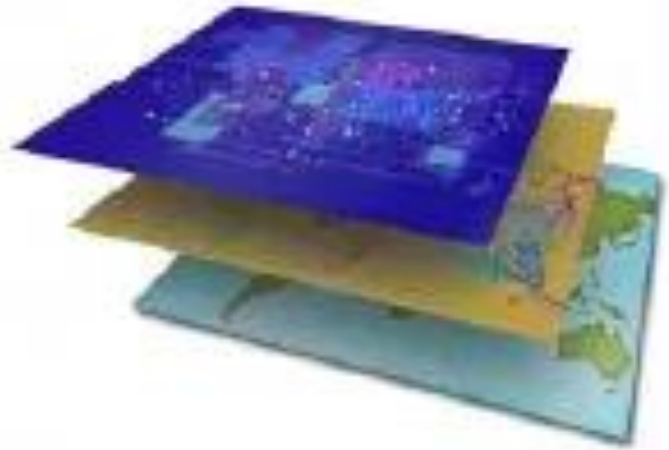
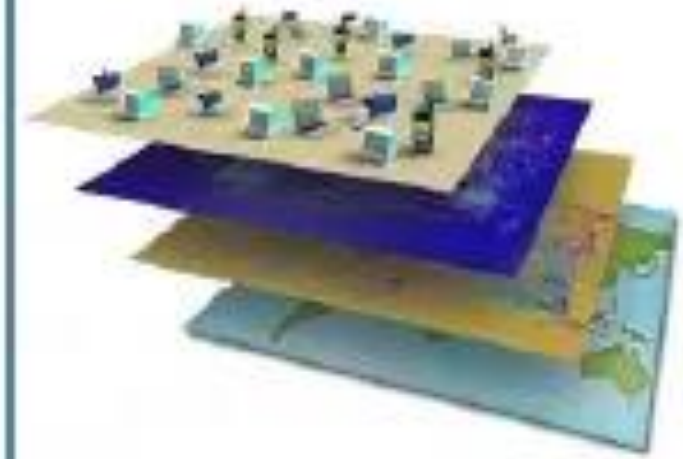
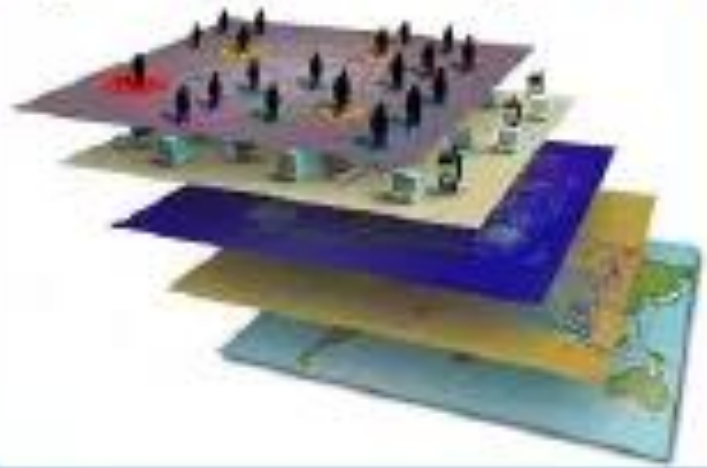
Picture source: https://www.shutterstock.com/image-vector/high-expectations-monitoring-scale-illustration-template-1283008774

Talking About the Same Thing …



- Domain of operations: mindset, ever contested
- Cyber incident v. cyber attack
- Critical National Infrastructure (CNI) and information sharing
- Cyber is not a noun
- Layers of cyberspace: Physical – Logical – Social
- Hybrid Threats: Cyber effects as an enabler for other effects or …
- Defender's dilemma

Picture source: https://www.freddaviscorp.com/terms-and-definitions-efficacy-vs-efficiency/

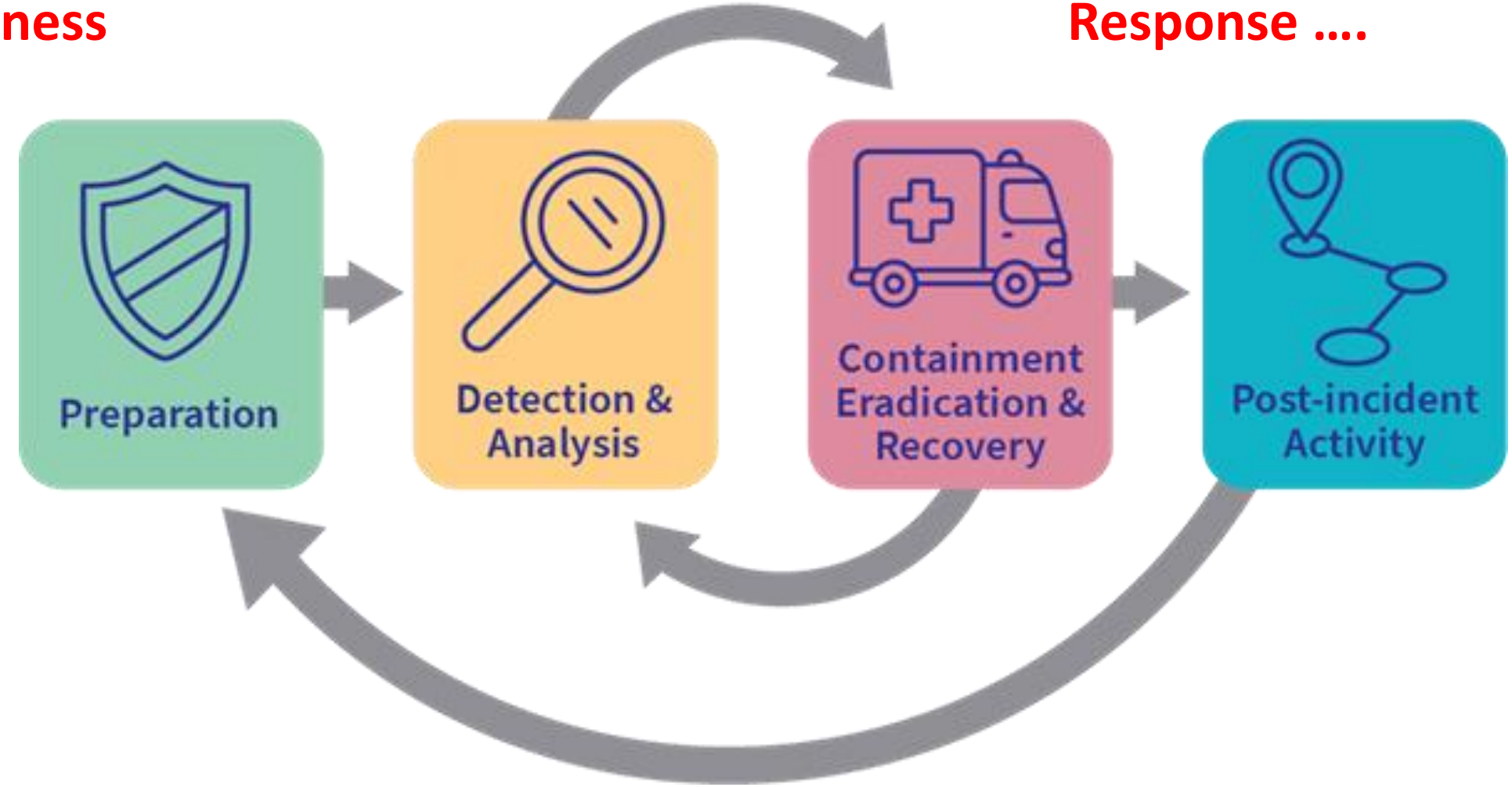
Physical Layer	Logical Layer	Social Layer
Geographic Components	Logical Network Components	Persona Components
		
Physical Network Components		Cyber Persona Components
		

Source: https://acqnotes.com/acqnote/careerfields/cyberspace

Cyber Incident Response Cycle

Readiness

Response ….



Source: https://axaxl.com/fr/fast-fast-forward/articles/cyber-incident-le-cycle-de-vie-de-reponse

Excursion: Deterrence in Cyberspace?

(From old ‘nuclear thinking’)

Demonstrate:

- Deterrence by **denial**
- Deterrence by **punishment**

*+ Deterrence by **attribution***

Attribution is a political (nation state) decision and much more than a technical exercise.

Perception, *“No response in kind”*

Picture source: https://www.frstrategie.org/en/publications/recherches-et-documents/causes-peace-role-deterrence-2018
https://nsarchive.gwu.edu/briefing-book/cyber-vault/2021-04-26/diplomatic-domain-evolution-diplomacy-cyberspace

What Can We Do? Good Practices

- **Situational Awareness**
- Be **prepared** (Cyber incident response plan)
- **Continuity**: PACE Plan (Primary – Alternate – Contingency – Emergency)
- Resilience through redundancy costs money.
- “Analogue resilience”? (Process independence, org measures)
- “Let’s not take it for granted.” – Zero Trust, Defence in Depth
  - Proper (software) engineering

CCDCOE

Picture source: https://hope.be/hope_working_area/medical-devices/croos-border-cooperation/

What Can NATO Do?

- (Military) Instrument of Power
- Perspectives: NATO as an organisation v. NATO as an alliance
- Taking care of its own (organisation/Enterprise) systems and networks
- CNI is mostly in the hands of the private sector – national legislation
- Cyber Defence Pledge
- Core Tasks: Collective Defence – Crisis Response – Cooperative Security
- Information and Intelligence Sharing
- Mutual assistance between Allies
- Support from NATO as an organisation (capabilities / capacity)
- Articles 4 and 5 of the Washington Treaty
- …

Ideas From CCOE Hybrid Seminar, Oct 2021

(Presentation Chris Kremidas-Courtney)

- Resilience as deterrence
- Hybrid is a way to achieve political objectives “on the cheap.”
- Detect, Attribute, Respond, Recover
- You can’t surge a relationship
- Attribution is the sovereign decision of the host nation (to include public messaging, etc)
- Once a crisis begins, the resiliency you’ve built already is what you’ll have to work with

Ideas From CCOE Hybrid Seminar, Oct 2021

(Presentation Chris Kremidas-Courtney)

What can CIMIC/CMI do?

- Key role in Military Support to Civilian Authorities
- Key role in building resilience
- Assisting with detection and attribution
- Assisting with response and recovery
- Assisting with strategic messaging

Role of NATO Force Integration Units (NFIUs)

(Presentation MNC NE)

What can CIMIC/CMI do?
Is Cyberspace Perhaps Different?

- Different standards in traditional domains (Land, Sea, Air)
- Where does CIMIC/CMI come from?
  - Primed by stabilisation/peacekeeping missions?
- CNI: Liaison with public and private sector entities?
- “Militarisation of cyberspace?”