Seminar Series Resilience in the Cyber Domain – Meeting Minutes

Format:	Expert Talk
Moderators:	Major Ralf Baur, Commander Rene Halfmann
Experts:	Colonel Dr **Josef Schroefl** (The European Centre of Excellence for Countering Hybrid Threats) Mr **Jiro Minier** (German Cyber Security Organisation GmbH) Lieutenant Colonel **Axel Haas** (Supreme Headquarters Allied Powers Europe)
Audience:	Open to the public. Practitioners, experts, academics, and advanced students
Date:	10 FEB 22, 15:00 - 17:00 UTC+1
Duration:	120 min

Guiding Questions:

- 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?

Expert: Colonel Dr Josef Schroefl
Title: Cyber as main enabler of Hybrid Threats

1. **Threat environment drivers:**
   - Globalisation and the changes in world order
   - New technologies play a special role
   - Increasing strategic competition
   - Role of COVID-19

   -> We are dealing with increased complexity
   -> All new technologies take less time to gain followers and have their relation to "cyber"
   -> Increasing degree of crosslinking
   -> Decreasing understanding of the architecture

2. **What are we dealing with?**
   - Cyber Crime (ransomware)
   - Cyber Espionage, i.e., attacks to steal vaccine research
   - Disinformation (Deep fakes, "trolls") i.e., actions against EU and NATO by trolls accusing "Russophobia", pro-Putin comments, using proxy servers

- Cyberwar i.e., Case Study: Israel vs Iran in Summer 2020, first Iran is being linked to an attempted cyberattack against Israeli water supplies; Israel is linked to a disruptive cyberattack on Iranian port facility
- Propaganda/fake news
- Strategic levels
- Support funding
- Cyber tools
- Economic leverage
- Proxies
- Asymmetric warfare

3. **Hybrid Influencing : China appears to warn India**
    - Early summer 2020, Chinese and Indian troops clashed in rise border battle in the Galwan Valley bashing each other to death with clubs; later in October 2020 in Mumbai/India the whole electricity blacks out after China posed a warning
4. **Archetypes of Hybrid Warfare: Vietnam 1968**

5. **Is there a counterpart to Hybrid Warfare?**
   -> Military Centric Warfare as in the Falkland war

6. **Hybris Warfare case study: civil war in Ukraine**
   - Since 2014: (cyber & kinetic) war between Russia and the Ukraine; Ukraine as Russia's test lab for hybrid war

7. **Environment of hybrid crisis**
   - Preparation starts in peacetime,
   - Destabilisation begins in phase II, when the actor and goal becomes clear
   - Phase III use of military
   - Phase IV negotiation

8. **Hybrid CoE Project: Cyber Power in Hybrid Conflict/Warfare**

   Outcome:
   - NATO and EU have established a good basis to counter cyber and Hybrid Threats
   - Cyber became a part of collective security
   - National cyber crisis management mechanisms could be used also against Hybrid Threats

9. **Are Cyber and Hybrid the same? What is "Cyber" now in context to Hybrid Threats?**
   - Cyber attacks are only a part of hybrid threats
   - Cyber space is a domain and there is no hybrid domain
   - Cyber attacks are tools to achieve strategic goals
   - Cyber space is the main enabler for hybrid threats

10. **Responding to Hybrid Threats**

ENDS: resilience and deterrence
WAYS: comprehensive and integrated approach, democratic processes and structures
MEANS: preparedness, capabilities, legislation, communication

Expert: **Jiro Minier**
Title: **Cybersecurity, Hybridity, and Resilience: A practical and conceptual overview**

1. **Setting the Stage - challenges in cyberspace**

- 2021 exemplified the current state of cybersecurity in public and policy discourse i.e., cyber espionage: SolarWinds incident, Microsoft Exchange Server incident; Ransomware: Colonial Pipeline incident
- 2022 - Beyond the headlines - speculation and thinking regarding what this might look like and what this might mean, i.e., ongoing Russia-Ukraine stand-off: what might the cyber activity look like as the crisis escalates?
- Lack of clarity as to how scenarios might play out in the cyberspace

A complex cybersecurity landscape
- Cybersecurity as a double strategic disappointment
- Cybersecurity more as ecosystem than war fighting domain

2. **Hybrid Threat? Is Cybersecurity relevant to Hybrid Threats**

- yes.
- Characteristics of Hybrid Threats:
-> Actor diversity, exploitation of grey zone ambiguity between war/peace, strategic impact beyond warfare, Hybrid Threats go beyond what is traditionally known as “hybrid warfare”

- Hybrid warfare vs Hybrid Threats
- Cybersecurity lives and breathes “hybridity”

3. **Conceptualising resilience**

- Cybersecurity and cyberspace is crucial to resilience
- 7 baseline requirements for national resilience from the 2016 Warsaw Summit can and have been challenged within the cyber domain i.e., resilience of transportation systems - recent cases in Iran and Belarus
- Resilience thinking and planning is also central to contemporary cybersecurity - cybersecurity is no longer enough, cyber resilience is needed
- What should be done? - communication and education surrounding cybersecurity and understanding inventories, connections, dependencies.
- Essential: what happens after the intrusion?

4. **Considering Approaches**

- The task distribution challenge
- How to tackle hybridity?

Meaningful cooperation and information sharing - good in theory, harder to implement effectively

Expert: Lieutenant Colonel Axel Haas
Title: Resilience in the Cyber Domain

1. **Terms and definitions**

- In general, it is important to have the same understanding of terms and definitions in this topic, which is often only an assumption that should be verified

Cyberspace as domain of operations for different actors; everything is connected

- Different types of Cyber-activities:
  - Cyber espionage
  - Cyber incident
  - Cyber attack, which is not clearly defined and may mean anything from any offensive cyber effect to one the results of which equal those of an armed attack
- Cyber should not be used as a noun
- Critical National Infrastructure and information sharing
- To analyse the effects of cyber activities it is appropriate to consider them on the physical, logical and social layer following various layer models in literature and doctrine
- Hybrid Threats: Cyber activities can stand alone, but they are usually embedded in other extensive operations and thus part of the puzzle, mostly as an enabler.
- Defender's dilemma – The attacker needs to succeed only once, while the defender must always succeed
- Therefore, the general approach is to be as resilient as possible, but this costs resources and should be considered in a risk management approach. Further, as we should work with the assumption that an attacker has already managed to break in, or will likely manage, we should prepare for the following step(s) in line with Jiro’s presentation.

2. **Cyber Incident Response Cycle**

- There are different Models, this a Standard Model
- Preparation
- Detection & Analysis
- Containment Eradication & Recovery
- Post Incident Activity

3. **Deterrence in Cyberspace?**

- Deterrence in Cyberspace is contested thinking, but in general applicable

  There are different forms:
- Deterrence by denial
  - The attacker is deterred by defensive capabilities that are too strong and make an attack too expensive or not worthwhile.

- Deterrence by punishment
    - The aggressor is deterred by retaliatory measures, which do not have to be ‘in kind’ (i.e., through cyberspace) but require confidence in the attacker’s attribution
- Deterrence by attribution
    - The attacker is deterred by public attribution (‘name and shame’)

4. What can we do?

- Develop Situational awareness as the foundation for taking informed decisions
- Be prepared, develop response plans
- Mission/Business Continuity Management, e.g., develop PACE Plan
    - Enhancing Resilience through redundancy costs money and resources
- “Analogue Resilience” be independent as you can be from cyberspace assets
- “Let's not take it for granted” contested environment: you need to be prepared. Layers of defence, make it more difficult for the intruder

5. What can NATO do?

- Military Instrument of Power
    - Always the question: what can the MOP reasonably to?
- NATO as an organisation and NATO as an Alliance
    - NATO as an organisation must protect its own IT systems
    - Alliance: NATO as an alliance has limited room for manoeuvre in the cyber arena as the protection of Critical National Infrastructure this is the responsibility of the member states
        - The Cyber Defence Pledge of the member states does exist, but it is a voluntary commitment
- Options: Share information and intelligence
- Mutual assistance between allies
- Support from NATO as organisation
- Articles 4 & 5 of the Washington Treaty – BUT these are decisions consensually taken at the political level

6. Ideas from CCOE Hybrid Seminar

- Resilience as deterrence
- Hybrid activities are a way to achieve political objectives without using to many resources
- States need to be able to Detect, Attribute, Respond, Recover from Cyber-activities
- Intelligence and information sharing is about building relationships
- Attribution is the sovereign decision and right of the host nation, this is not a topic for NATO as an alliance

7. What can CIMIC do?

- Military support to civil authorities
- Building resilience
- Assisting in detection and attribution
- Response and recovery

- Strategic messaging
- Role of NFIUs

8. Is Cyberspace different?

- Different from traditional domains
- CIMIC / CMI is influenced by stabilisation and peacekeeping missions during the last 20 years – what is the role in collective defence?
    - Liaison with public and private sector entities could be an idea
    - Coordination dilemma everyone wants coordination but no one wants to be coordinated
- “Militarisation of cyberspace” should the military take over? It's question of capabilities/ capacities, but also with legal and ethical implications