The Military Role in Cyberspace

Major General Wolfgang Renner
Deputy Chief of Staff Cyberspace
Supreme Headquarters Allied Powers Europe (SHAPE)
Our Political
Economic
Social
Personal
Lives
Legal
Commercial
Media
Military
Systems

Are Increasingly Dependent Upon Cyberspace
Our Political, Economic, Social, Personal Lives, Legal, Commercial, Media, Military Systems Are Increasingly Dependent Upon Cyberspace

Cyberspace Defence IS A Matter of Collective Defence
Cyber Defence Pledge

Cyberspace as an Operational Domain

Decision to Establish the Cyberspace Operations Centre (CyOC)
Two Fundamental Considerations

1. Integrating Cyberspace into Joint Operations
2. Addressing the Unique Aspects of Cyberspace
Cyberspace Operations Centre

• **Mission:**
  – Provides persistent, centralized and comprehensive cyberspace situational awareness
  – Provide cyberspace domain aspects of mission assurance
  – Focal point for the preparation, planning, conduct and coordination or execution of cyberspace operations
Integrating with Joint Operations: Cyberspace Directorate

- SHAPE COS
  - DCOS: Strategic Employment Directorate
    - Campaign Planning & Joint Effects
    - Director CyOC
      - Deputy Director CyOC
      - Situational Awareness Branch
      - Operations Branch (CLES)
      - Plans Branch
  - ACOS J6 Cyberspace Division
    - Twinned Post
    - Commander NATO CIS Group
  - CCOMC

- SACEUR

Cyberspace Operations Centre:
- 66 staff
- 44 offsets have been identified from SHAPE Cyber and J6 Divisions,
- 22 further offsets or new PE posts needed

Cyberspace & CIS Domain Advisor
FMN: Co-ordination on the capability and integration
(Possible future cyberspace CFIT)
1 Integrating with Joint Operations: Planning and Execution

Established Operational Planning Process

Cyberspace as an Operational Capability

NATO Crisis Response Process

- Indications and Warnings
- Assessment
- Response Options Development
- Planning
- Execution
- Transition
Two Fundamental Considerations

1. Integrating Cyberspace into Joint Operations

2. Addressing the Unique Aspects of Cyberspace
Adapting to Unique Aspects: Persistence

- Cyber Defence has to be a “Day Zero” capability
- Everyday cyber incidents offer opportunities for collaboration and learning
- Effective NATO-National coordination requires regular practice through exercises and training
Adapting to Unique Aspects: Proactivity

- Cyberspace is the newest and most dynamic domain of operations
- We cannot rely on a body of tested doctrine, techniques, tactics and procedures
- Our operational stance has to be agile, adaptive and collaborative

All of Us are Smarter than One of Us
Global pushback on Russian hacking as Dutch thwart cyber attack on chemical weapons watchdog

The United States charged seven Russians with hacking international organisations.

Russia must be held accountable for cyber attacks - Mattis

BRUSSELS (Reuters) - U.S. Defense Secretary Jim Mattis said on Thursday Russia must be held accountable for its attempts to hack the Organization for Prohibition of Chemical Weapons (OPCW).

‘Russia must stop its reckless pattern of behaviour’, NATO’s Stoltenberg warns

By Alexandra Brzozowski and Samuel Stolton | EURACTIV.com

Russia cyberattacks - live updates: GRU accused of targeting Dutch chemical weapons body and Porton Down

GRU also blamed for attacks targeting Foreign Office

NATO, UK and Netherlands lash out against Russian cyber attacks

ANI | The Hague [Netherlands] Last Updated at October 4, 2018 20:20 IST
Two Fundamental Realities

1. What Happens in Cyberspace Affects How We Fight

2. What Happens in Cyberspace Affects Our Collective Defence
SHAPE is Addressing the Challenge