Cybersecurity & cyber defence:

Strengthen Cyber Resilience & EU Cyber Market

PhD. Jorge Maestre Vidal

Senior Specialist in Cyber Defense

jmaestre@indra.es

Dual-Use Technologies 2022

Cybersecurity & Digital Applications in Defence

Málaga, Nov 17-18 2022 @DEFIS_EU @IDEAJUNTA #ENDR

Growing Challenges, but not New Ones

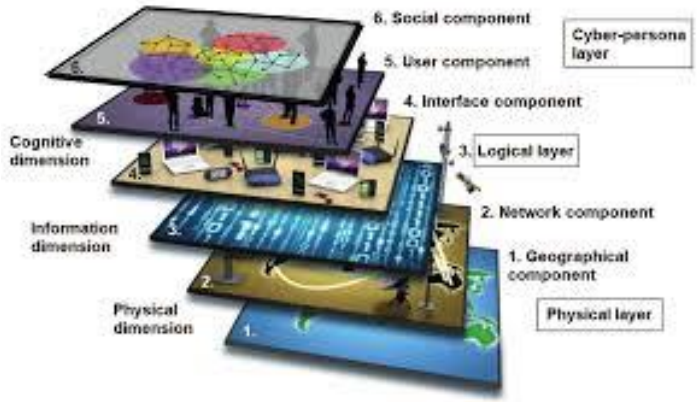
- In 2018 EU identified cyberspace as a domain of military operations. The 'Military Vision and Strategy on Cyberspace as a Domain of Operations' adopted in 2021 sets the framework conditions and describes the ends, ways and means needed to use cyberspace in support of the Defence Policy (CSDP) operations

- **Shoulde be able to address a situation comparable** in scale and intensity when conducting the full spectrum of military tasks
- How to **adjust upward** the existing collaborative instruments and processes, to help Member States **develop capabilities "at scale**
- Reducing the EU's **strategic dependencies in critical cyber technologies** and strengthen the European Defence Technological and Industrial Base (EDTIB)
- Need to establish an EU Cyber Defence Coordination Centre (EUCDCC) supporting **enhanced situational awareness**
- MICNET should serve enable **information-sharing among the different levels within the cyber defence community**
- **EU Cyber Solidarity** for stronger common detection and situational awareness

Duality is a “Privilege” not a “Right”

- Most cyber security solutions do not meet the duality requirement, or need significant improvement.
- Huge gap between native needs (operational planning, cyber c2 etc.) and the dual use spectrum.

- Minimal understanding of cyberspace as **fifth battle domain**
- Understanding cyberspace in **multi-domain** operations (eg. New FM 5-0)
- Minimal understanding of cyberspace at **full spectrum** (eg. EU CIDCC)
- Minimal understanding of **state-level implications** of COs
- Minimal understanding of **COs in a conflict** (integral deterrance, escalation from competition, crisis, etc.)
- **Constantly evolution of doctrine**, SOPs, etc.
- Minimal understanding of **COs in a coallition** (FMN, ToAs, etc.)
- Anticipate to growing war concepts: **SoS, Mosaic Warfare,** etc.
- **Future Needs**: active defene, deterrence, assistance to SCEPVA, etc.



Raising topics on which we needed to think

- EDTIB needs a **cybersecurity risk-management programme** that includes supply chain security as well as incident reporting
- **EU cyber defence interoperability requirements** (ongoing by EDA, EUMS)
- **Technology roadmap for critical cyber technologies** (ongoing by EC, EDA and cMS).
- **Foster non-dependences** in critical technologies
- **Roadmap to strengthen European industrial capacity** in cyber defence, including specific capability objectives and relevant funding instruments
- Promote the development of a '**European trusted supplier' certification** framework for suppliers throughout cyber supply chains, which should include European non-EU countries and be compatible with the US DoD's Cybersecurity Maturity Model Certification framework

The Human Factor

- Skills and competences are essential to overcome strategic dependencies on cybersecurity and cyber defence in Europe, but also the support of the EU Citizens

- The European workforce needs to **retain key skills and acquire new ones**
- **A lack of skills** has a negative impact for the defence sector, as it hampers capability development in all domains
- **Lack of sectorial skills and short-term learning strategies**
- **Embrace Multidisciplinary**. Engineers shall not work alone
- **Debunking AI** and other trending competences
- **Harmonized specifications, accreditations and competences** in CD
- The **Dual-use dilemma**. Social perception of dual-use as threat
- The **Digital Bubble and Long term professional development**
- Prompt **defence culture and collaboration with Academy**

You go to war with the army you have, not the army you might want or wish to have - Donald Rumsfeld