EUROPEAN DEFENCE AGENCY



Pooling & Sharing Opportunities

Mario Beccia, Cyber Defence Programme Manager

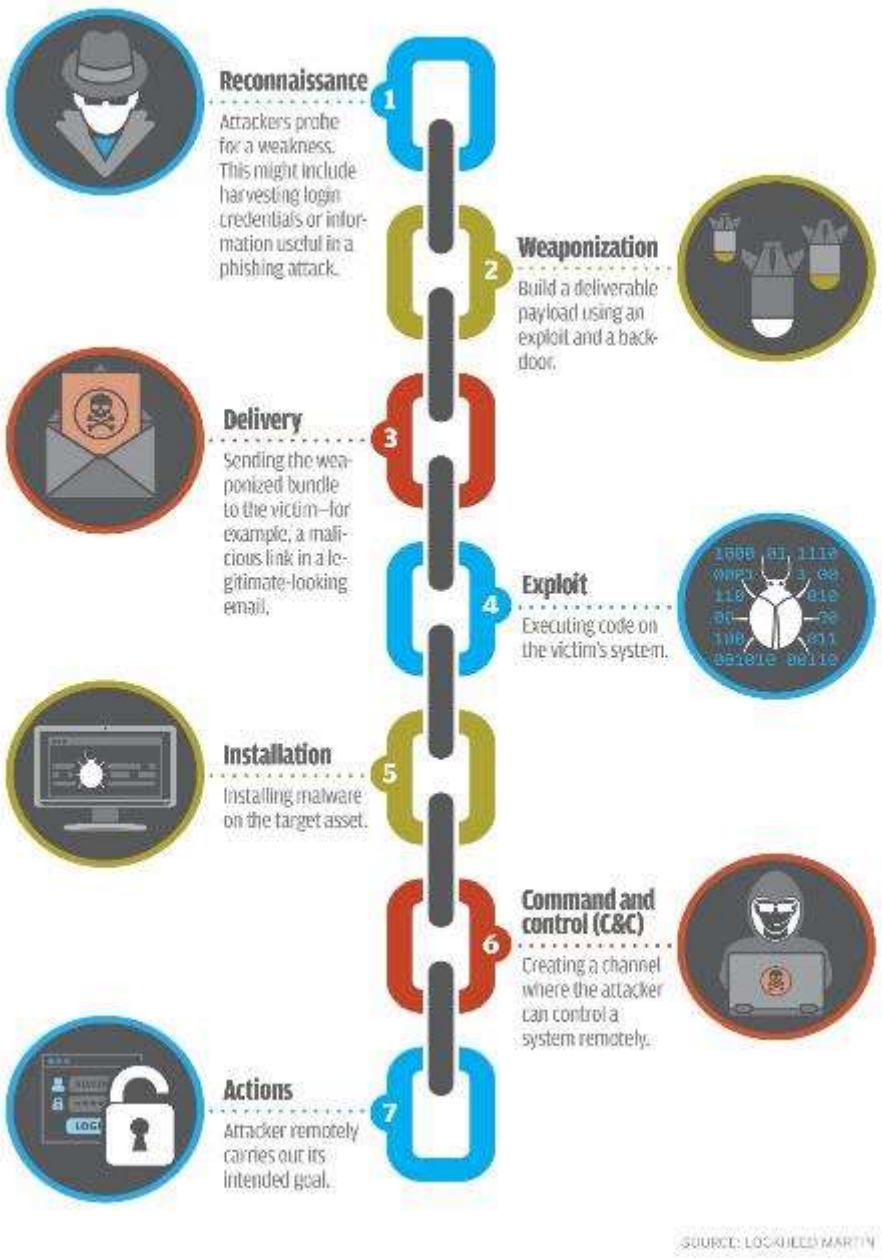
April 19th 2018

Have you ever met this guy?



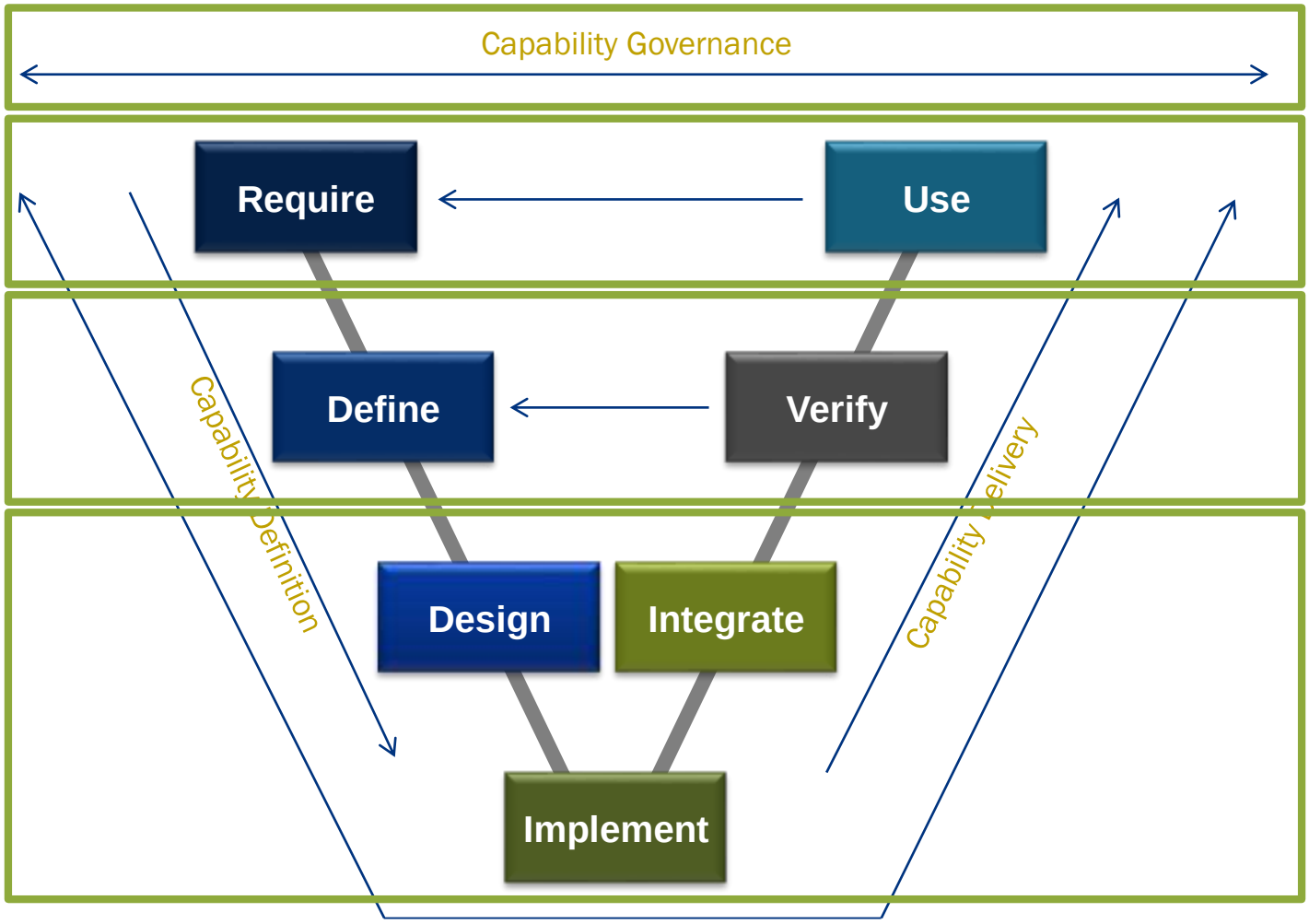
The Cyber Kill Chain

- Cyber attack tools are assembled on-purpose, but starting from existing libraries and lower level tools
- Attacks require a *long preparation*, *dedicated skills*, *dedicated tools*
- Any sophisticated attack requires a *complex mix of tools, skills and people*



→ Pooling&Sharing (of knowledge, capabilities, people, processes, etc…) has been long exploited by attackers

On the other side



What is essential in war is victory, not prolonged operations (**harmonize goals**)

Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win (**use common design and architecture**)

We cannot enter into alliances until we are acquainted with the designs of our neighbors (**interoperability and exercises**)

Speed is the essence of war (**development and innovation**)

(loosely based on Sun-Tzu's The Art of War)

Active projects with Pooling&Sharing potential

- Cyber Defence Training and Exercises Platform (CDTEXP)
- Cyber Ranges Federation
- Cyber Defence Strategic Research Agenda update
- Supporting PESCO Projects:
  - Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (PESCO 8.1, led by Lithuania)
  - Cyber Threats and Incident Response Information Sharing Platform (PESCO 6.5, led by Greece)

The power of collaboration…





Thank you!

Backup Slides

EDA's Reinforced Mission



In May 2017, after EDA's **Long Term Review,** Defence ministers **reinforced** the Agency's mission:

- as main instrument for intergovernmental capability planning & prioritization
- as the prime forum and coordinator for the whole lifecycle of capability development
- as Member States' central interface & gateway towards EU institutions & stakeholders

Cyber Defence Programme ambitions

- Education, Training, Exercises and Evaluation
  - Support the ambition of Building a Successful Cyber Defence Workforce
- Cyber Defence Research and Technology
  - Ensure the availability of state-of-the-art Cyber Defence Technology, following our Cyber Strategic Research Agenda
- Cooperation and synergies with relevant actors across Cyber Cefence and Cybersecurity areas
  - Create and support collaborative relations with entities such as European Commission and NATO (under the NATO-EU JD)

Cyber Defence Programme ambitions

- Establish a Systems Engineering reference framework for defensive Cyber operations
  - Architectural products and frameworks provide a common vocabulary, technical, procedural and organizational guidance and standards advice from which interoperable capabilities can be implemented
- Address cyber defence challenges in capability environments (Air, Space, Maritime and Land)
  - Cyber Defence challenges extend to other military domains, where traditional focus areas (Command&Control, situational awareness, information sharing, etc…) can be affected by events in cyberspace