The CyberROAD roadmap

Enrico Frumento (CEFRIEL)
This presentation aims is to clarify the concept of roadmapping and show how it was used in CyberROAD.

We all live in a world that is constantly shaped by several driving forces, which are paving the road to the future.

A roadmap is the method used to identify these forces, understand their influence in today’s and tomorrow’s world.

Cybercrime and cyberterrorism are special because are influenced by external (e.g., defence strategies, business, social, political, legal and technological) and internal forces (e.g., evolution of malware, black market, RCE).
What is a Roadmap

The viewing angle through which interpret the evolving phenomena of the World at a given time and its possible evolutions.

Examples: Healthcare, Transportation, Future of Networking, Automotive, Critical Infrastructures …
What is a Roadmap

How we imagine the specific “aspect” of the world to evolve in the next years?
DO YOU REMEMBER DISNEY’S THEME PARK TOMORROWLAND?

SCENARIO (T1)
What is a Roadmap

Building a Roadmap means ..
- go deep into a specific scenario
- understand which are its pillars and driving forces
- understand which are its specific threats today and tomorrow
- figure out how it will be in 2024 and how threats will evolve

HENCE
connect the dots ..
How countermeasures must evolve to face tomorrow's threats
What means gap analysis: threat at different moments in time

The aim of GAP Analysis is to track the changes in the threat landscape to improve defences

Threats today

- Increased threat (>)
- Decreased threat (<)
- Unchanged threat (=)
- Disappearing threat

Threats tomorrow

- New threat (!)

GAPs

\[t1\] \rightarrow \[t2\]
Toward the final Roadmap

- GAP
- Key factors for change
- Action Plan
Toward the final Roadmap

Gap analysis for every scenario

Gap clustering
Identification of common gaps across different scenarios (same gap in different contexts)

Research topics identified
High level grouping of gap clusters

D3.3
Social economic Legal research topics

D5.6
Cybercrime research topics

D6.6
Cyberterrorism research topics

D2.2
Risk assessment ranking methodology

Research topic ranking
Prioritization of RT on the basis of a risk metric

Research Actions
The final result of the project and concrete suggestions for future research focused on specific domains
• **Asset**: anything that has a value to the organization
• **Threat**: a potential cause of an unwanted incident which may result in harm to the organization
• **Vulnerability**: a weakness in an asset which can be exploited by a threat.
• **Risk**: the potential that a given threat will exploit vulnerabilities of an asset to cause loss or damage to the asset.

• We considered several types of risk:
  – Data Breach Risk
  – Health & Safety Risk
  – Financial Risk
  – Intangible Risk
When now then have

• A clear understanding of what is a roadmap and why cybercrime and cyberterrorism are «special»
• A set of gaps grouped into Research Topics
• The corresponding Research Actions needed to fill the gaps
• A definition of the Risks that we want to measure
• A ranking method

Just apply the method and find a good graphical representation
Research Topics readiness

- The area **covered** by the radar graph is the **readiness** of current defences in the 4 considered directions.
- The area **outside** the radar graph is the gap that needs to be filled by the **research**, to reduce the risk

**The greater is the occupied area, the better are the current defences**
COURAGE, CAMINO and CyberRoad
Consolidated Research Roadmap
Ladies and gentleman ...