National resilience to cyber-warfare

ANA-MARIA MATEJIC

Cyber-security advisor

Ibis Instruments
Measurement & Telecommunication Systems

From cyber-security to cyber-resilience

- Cyber-resilience
  - A natural thing
  - A cultural shift
  - A step ahead for businesses to recognize that hackers have innovative tools, elements of surprise and *can be* successful in the attacks carried
  - Being ready for everything is the “heartbeat” of cyber-resilience

Key challenges in “national cyber-resilience”

- At first it was : can we have a “national” kind of cyber-resilience ?
- Supported by the international context:
  - More connected but more vulnerable
  - New types of attacks are about businesses (€) but mostly they are about inducing “fear” to the people
  - Worldwide : more devices than people
  - Attacks can target one country but side-effects touch other economies
- Setting up the “cyber-security strategy” followed by an effective oversight
- Protect the C-I-A triad at the “national” level

The warning has been given

"Cyber threats will pose an increasing risk to public health, safety and prosperity as information technologies are integrated into critical infrastructure, vital national networks and consumer devices."

(***US National Intelligence Strategy Report***, January 2019)

It’s about starting it …

- A “defense in depth” or/and “zero-trust” approach ?
- Does “left” know what “right” does ?
- Risk-governance
- Communication in public-private partnership
- Tailor-made solutions
- Roadmap
- Remember : it’s a cultural thing

Thank you and let's work on it