THE SECURITY OF CRITICAL INFRASTRUCTURE AND PUBLIC SPACES IN THE EUROPEAN UNION

The prospective incidence of Terrorism on Cyber Security

European Parliament in Brussels, 12 July 2018

WWW.LARSHILSE.COM

Global Thought Leader in #DigitalStrategy, #CyberSecurity, #CyberTerrorism, #CyberDefence, #CyberCrime

Terrorism

Political violence in an asymmetrical conflict that is designed to induce terror and psychic fear through the violent victimisation and destruction of noncombatant targets.

Current Understanding of Internet Usage for Cyber Terrorism (Based on Academia)

- Communication and Networking
- Asset Transfer
- Research about Targets // Espionage
- Recruit Supporters for the Groups Cause & Raise Funds
- Propaganda // PsyOps

What’s up with the Deep Web?

Threat Vector Categories

- Cyber only Attacks
- Cyber-Physical Attacks
- **NEW** Kinetic Attacks with Cyber Consequences

Academic Recommendations to mitigate the Risks

- Legislative Framework
- National & International (law enforcement) Partnerships
- Strategies

What really enables Cyber Terrorism?

- Reliance on the Internet for our society to function
- ISPs not regulated (Network Infrastructure not redundant, etc.)
- Software/OS Vendors releasing premature Products
- Gross negligence in deployment, and continuous update/upgrade of critical infrastructure hard-/software
- Failure of the Legislative Branch since the 1980s

Reality Check: 2-Phase Approach

- Phase 1: Immediately create Task Force to establish a qualified Threat Landscape > hardening of Critical Infrastructure in the EU

- Phase 2: Creation of legislative Framework making liable those elements identified as enablers for contributing factors (software/OS Vendors, IoT device Manufacturers, CTOs, etc.)

Questions? Reach out today!

WWW.LARSHILSE.COM/GO/CONTACT **Phone** +49 (0)4835 9513027 **Email** lars.hilse@gmail.com
PGP Fingerprint 44D5 68A1 32A1 AD87 3E29 2AA2 9B4A 1674 17FF C660