CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Ten. Col. CC Felice DE LUCIA
JFCNP OPS J2 CJ2X Head

CYBERDEFENCE IN NATO

Cyberspace as DOMAIN - Recognized at WARSAW SUMMIT

Cyber Defence Organisations within NATO

- **Policy, Directive & Guidance:**
  - NATO Security Committee (NSC)
  - Defence Policy and Planning Committee (DPPC)
  - NATO C3 Board (NC3B)
  - NATO Military Committee (NAMILCOM)
  - NATO Cyber Defence Management Board (CDMB)

- **Operational & Technical:**
  - SHAPE & SACT NATO CIS Security Accreditation Board (NSAB)
  - NATO Emerging Security Challenges Division, Cyber Defence Section (ESCD CD)
  - NATO Computer Incident Response Capability Coordination Centre (NCIRC CC)
  - NATO Computer Incident Response Capability Cyber Threat Assessment Cell (CTAC)
  - NATO Information Assurance Technical Centre (NIATC)
  - NATO Computer Incident Response Capability Technical Centre (NCIRC TC)
  - NATO C3 Agency (NC3A) / NATO C&I Agency (NCIA)
  - NATO CIS School (NCISS)
  - NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

What is Cyber

Computer Network Operations

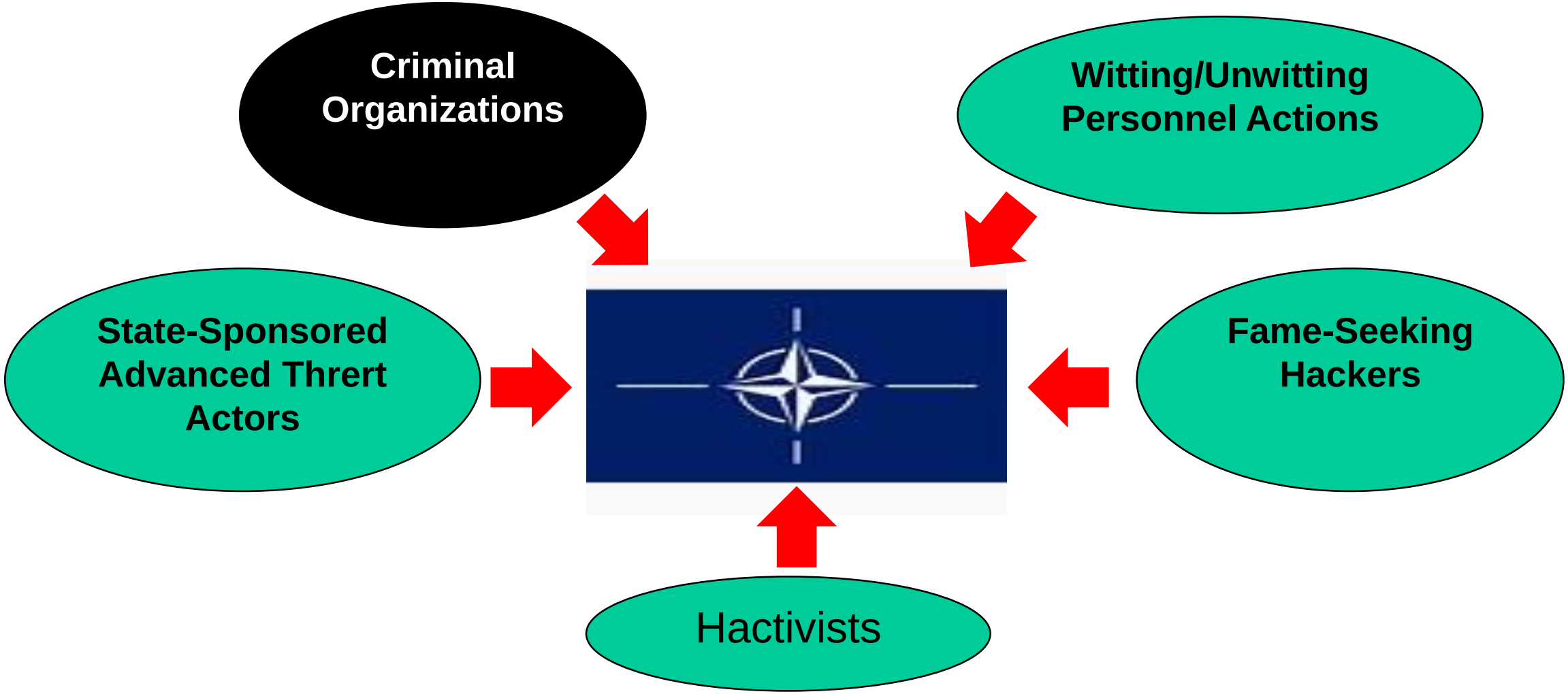
Cyber Defense

Cyber crime

Cyber warfare

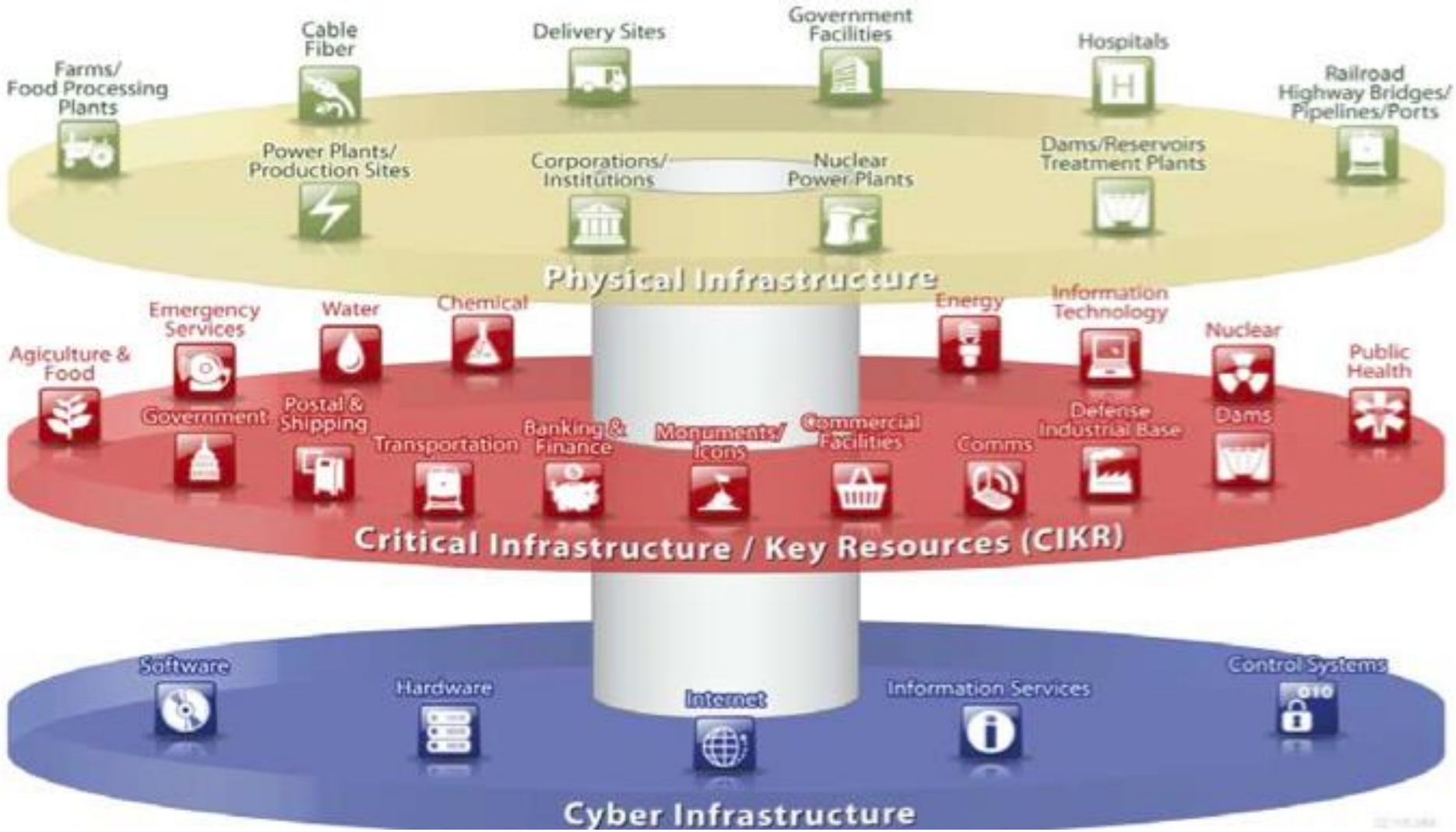
Hactivism

NATO is a Target



Cyber in Hybrid Warfare

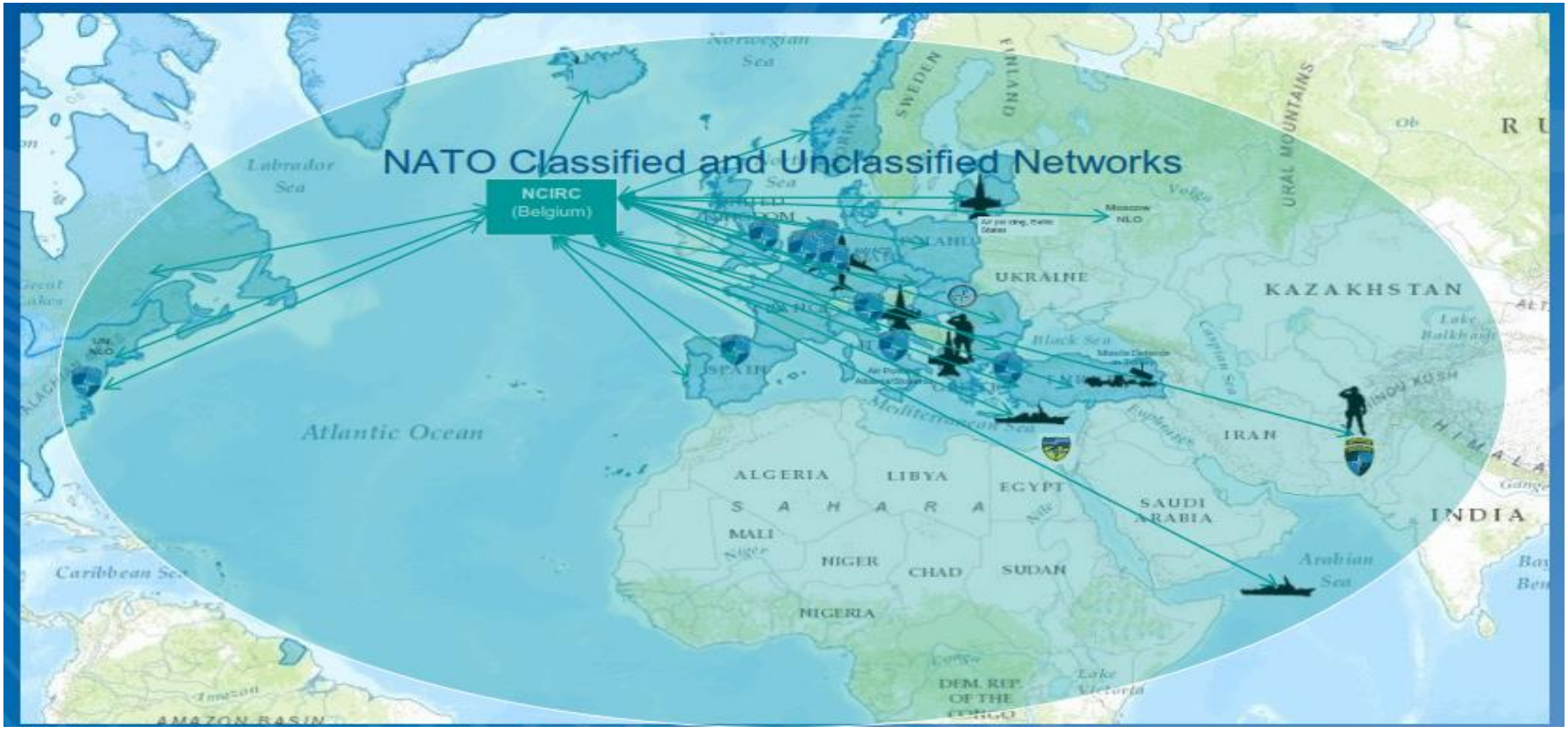
POSSIBLE TARGETS



NATO RESPONSE TO THE CYBER THREAT

- Centralized Protection of NATO Networks
- A centralised capability – the NATO Computer Incident Response Capability (NCIRC)
- Strategic level analysis with the Cyber Threat Assessment Cell
- Rapid Reaction Team deployment for NATO's own systems and, subject to Council decision on a case-by-case basis, for Allies
- Continuous evaluation of NATO's capabilities in view of rapid technological evolution.

Centralized Protection of NATO Network



NATO Global Response to the threat

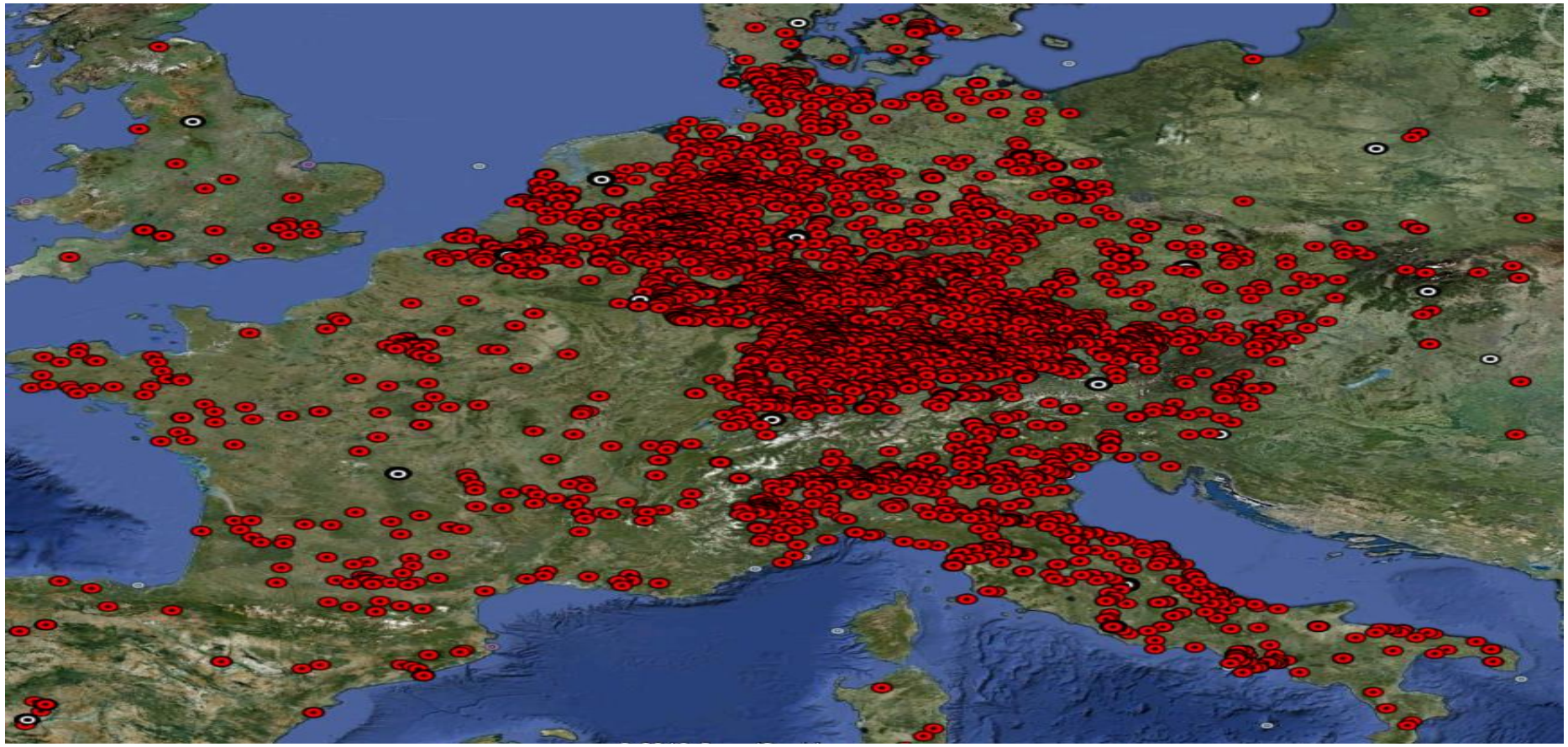
29 Member Nations

40 Partner Nations

CRITICAL INFRASTRUCTURE DEFINITION

Although there is no universally agreed definition, critical infrastructure is generally understood as those facilities and services that are vital to the basic operations of a given society, or those without which the functioning of a given society would be greatly impaired.

CRITICAL INFRASTRUCTURE



RESPONSABILITIES

NATO CRITICAL INFRASTRUCTURE PROTECTION
NATO RESPONSABILITY through its Cyberdefence organization

COOPERATION

NATO NATIONS CRITICAL INFRASTRUCTURE
are responsible for their critical infrastructure

How to protect Critical Infrastructure

it is impossible to protect critical infrastructure fully against all types of threats

Risk management

Protection measures to reduce the risk

Risk assessment

- threat to the infrastructure
- vulnerability of the infrastructure

- expected consequences or impact on the infrastructure should that threat materialise.

Protection of the infrastructure

- physical protection measures
  - which target the physical components of an infrastructure
- electronic or cyber-protection measures
  - which aim to protect the ICT infrastructure against attacks
- human or personnel protection measures
  - which target the infrastructure's staff and other categories of people bearing some direct relation to the infrastructure
- organisational measures
  - which relate to the way the infrastructure is managed


CYBER WARRIORS
THE THREAT IS ONLY A CLICK AWAY
Become a member of a highly technical and skilled force to meet requirements in computer network defense and other computer network operations. Be on the front lines to engage the types of information technology and computer network cyber threats we face in 21st century as a Cryptologic Technician Networks (CTN) For more information visit navy.com.
AMERICA'S NAVY
A GLOBAL FORCE FOR GOOD.™

QUESTIONS?