Mandate related

26/04/2017

European Union Agency for Network and Information Security

Context

FRANCE 24
International News 24/7

TOP STORIES
VIDEOS
SHOWS
FRANCE
AFRICA
MIDDLE EAST
EUROPE
AMERICAS
ASIA / PACIFIC
SPORTS
BUSINESS / TECH
CULTURE
DOCUMENTARIES
IN DEPTH
INFOGRAPHICS
THE OBSERVERS

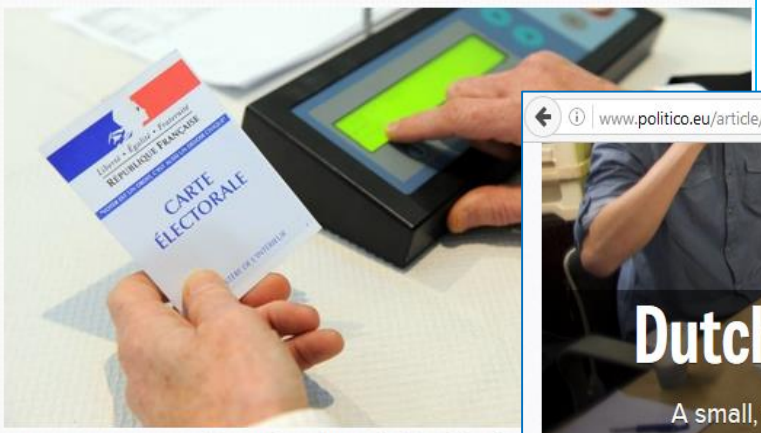
France Medias Monde | Watch us on TV | Travel | My account

WATCH LIVE 10:57 (Paris time) IN THE PAPERS

France | French Presidential Elections 2017 | hacking | cyber crime

France takes steps to prevent an election hack attack

Share 299 | Tweet | Share 0 | submit | Share 187



© Fred Tanneau, AFP | Electronic voting during local election
French port city of Brest on March 22, 2015

Latest update : 2017-01-16

**Alarmed by allegations of Russian me
2016 US presidential race, French aut
warned political parties against the th
attacks as the country prepares to ele
president in May.**

A US president-elect who may be compromised by a foreign power. A presidential election marred by cyber attacks, leaks and interference. An

theguardian

home › tech | UK | world | sport | football | opinion | culture | busin | all

Hacking

Smartphones, PCs and TVs: the everyday devices targeted by the CIA

Documents published by WikiLeaks reveal extent of intelligence agency's capability for targeting the public

WikiLeaks describe CIA using techniques 'to bypass the encryption' of a number of popular encrypted chat apps such as WhatsApp and Signal, in addition to exploiting a vulnerability in Samsung TVs. Photograph: David Paul Morris/Bloomberg/Getty Images

Alex Hern
Tuesday 7 March 2017 17.56 GMT

www.politico.eu/article/dutch-election-news-russian-hackers-ne

Dutch go old school against Russian hacking

A small, tech-savvy nation gives up on computers in this month's parliamentary elections.

By LAURENS CERULUS | 3/5/17, 6:49 PM CET | Updated 3/8/17, 8:10 AM CET

Early voters cast their ballot in a flower shop furnished as a polling station during Dutch local elections in Castricum in 2014 | Olaf Kraak/AFP via Getty Images

981 SHARES | 928 Shares | Twitter | 53 Shares | Email | Comment

THE HAGUE, Netherlands — Better safe than sorry.

Malicious intent – cyber attacks

Deliberate action(s)

- Development stage -> malicious logic
- Operational stage -> Intrusion

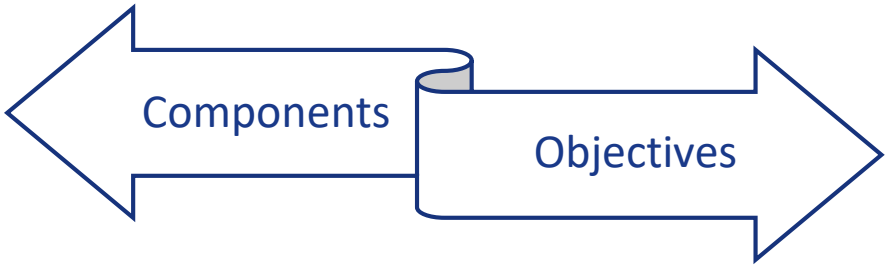
Using same infrastructure/networks/space

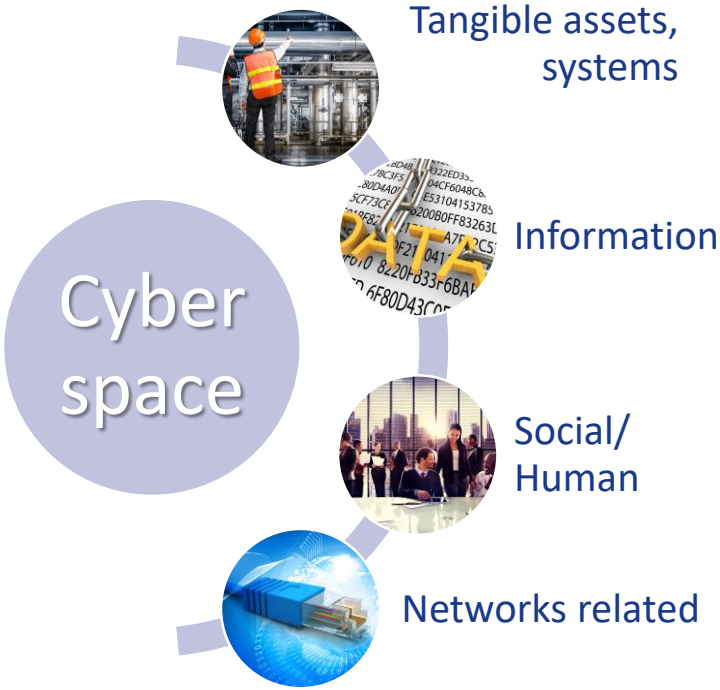
Targeting assets: systems/infrastructures/information/human

Exploiting weak links

*Cyber espionage » state espionage (intelligence, state actors) or industrial espionage (commercial actors)

Cyber security objectives





Dependability (of systems)

- Availability
- Reliability, Safety
- Confidentiality, Integrity
- Maintainability

Security (of information)

- Confidentiality, Integrity, Availability
- Accountability, Authenticity, Non-repudiation

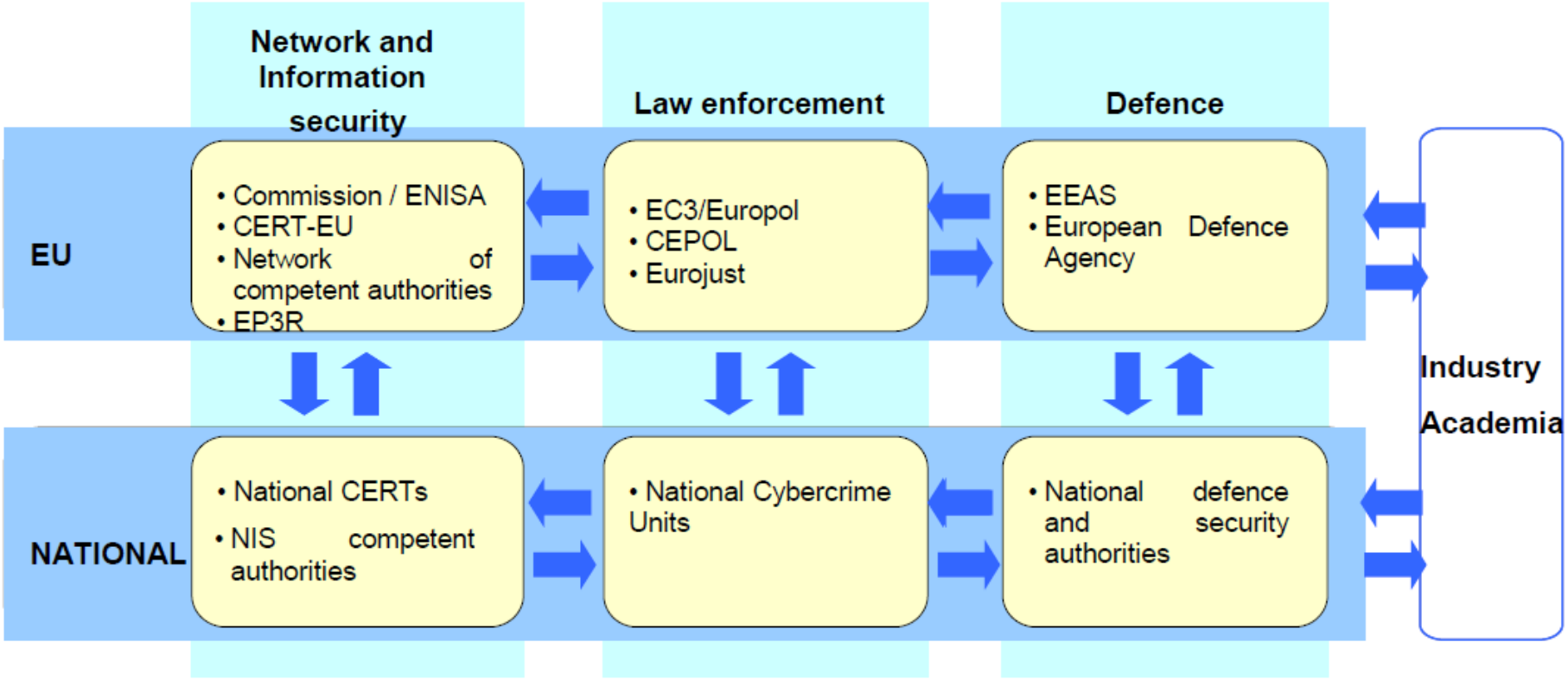
Resilience, Survivability, Robustness

European dimension

Review of

EU Cyber Security Strategy 2013

Need for a renewed EU cybersecurity governance (I)



*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

Need for a renewed EU cybersecurity governance (II)

✓ Covered by strategic objective
✓ Covered by ENISA work programme[1]
Global not only EU focused
Priority areas of overlap

		EC's strategy	ENISA's strategy	EUROPOL's strategy	CEPOL's strategy	EUCPN's strategy	CERT EU's strategy	EEAS's strategy	EDPS's strategy	BEREC's strategy	ITU's strategy
Ensure effective governance and coordination		✓	✓	✓					✓	✓	
Build situational awareness	Identification of critical assets		✓				✓				✓
	Identification of potential attackers	✓	✓				✓				✓
	Identification of vulnerabilities	✓	✓				✓				✓
	Balancing residual risk with risk appetite		✓								
Prepare and prevent	Law, policies and regulation	✓	✓					✓	✓	✓	
	Standards, guidelines and definitions	✓	✓	✓		✓	✓				✓
	R&D, education and awareness	✓	✓	✓	✓				✓	✓	✓
	Active defence		✓								
Withstand, recover and respond	Government facilitation and support	✓	✓	✓			✓				✓
	Direct government action	✓	✓	✓			✓				✓
Ensure efficient information sharing and cooperation		✓	✓	✓	✓	✓	✓		✓	✓	✓

1 work programme only assessed for ENISA activities

SOURCE: ENISA Work Programme 2015; EUROPOL, CEPOL and EUCPN strategy and work programme 2015

Topics to be consider during Cyber security strategy review

ENISA proposal

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in policy implementation
- ✓ Harmonisation across EU

COMMUNITY

Mobilizing EU communities

EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

ENISA evaluation. Drivers for change, SWOT analysis

Internal

Strengths

- **Landscape view** – unique position to analyse how all MS are doing and communicate back
- **Independence** – ENISA seen as an independent agency with no commercial or political bias
- A **facilitator** – ENISA focuses on collaboration and community-building
- **Needs-driven** – ENISA remains agile and able to respond to changing stakeholder needs
- **Cybersecurity excellence** – at several levels, covering the complete security lifecycle

Weaknesses

- **Growth** – pace of growth of budget and resources does not match pace of demand for ENISA involvement in new areas
- **Influence** – ENISA has limited influence over industry
- **Impact –** as with other EU institutions, ENISA needs a better methodology for tracking and understanding impact and addressing market needs

External

Opportunities

- **SPOC –** opportunity for ENISA to be the primary/coordinating EU cybersecurity body
- **Cybersecurity marketplace** – a role for ENISA in developing and supporting European cybersecurity products and services
- **Public-private partnerships** – ENISA could be supporting and developing PPPs, e.g. leveraging the results of research and exploiting opportunities for EU products and services in the cybersecurity market
- **Technology development** – opportunity for ENISA to be the reference body on cybersecurity implications from IoT, smart, mobile, AI
- **Privacy and data protection** –ENISA could be given a role in assisting MS and EU in addressing the technical challenges of implementing data protection

Threats

- **Fragmentation** – the EU cybersecurity policy space has no coherent governance structure that includes all EU players in a complementary manner
- **Strategic outlook –** difficulties in executing a long-term vision due to regulatory constraints and overlapping mandates (other agencies/bodies claiming to have expertise and ownership of cybersecurity)

Priorities / strategic themes
ENISA paper on *Cybersecurity beyond 2020*

Organic growth

- continuing the evolution of the functions of the Agency to address the latest cybersecurity challenges,

Policy advice

- provision of strategic policy advice to the EU institutions and MS in relation to cybersecurity,

Information and **capability-building**

- ENISA as the EU Cybersecurity Information Hub offering high quality cybersecurity analysis and training,

Cybersecurity lifecycle

- getting more involved in the complete cybersecurity lifecycle, including practical, "hands-on" support and an incident response (coordination) capacity,

Economics of cybersecurity

- including better engagement with industry to leverage economic opportunities in the EU from cybersecurity,

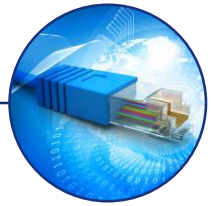
Standards and certification

- ENISA developing and promoting cybersecurity standards, managing certifications, or (possibly) evolving to a standardisation and/or certification body.

CYBER SECURITY GLOBAL SUPPORT

- Collaboration, Community building, Capacity building,
- CIIP, Network and information Security, Data Protection

Freedom, security and justice



Single market security

Cyber defense

Cyber diplomacy

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu