



ENISA in the future: Towards a new mandate and an actor in implementing the Cybersecurity Strategy of the European Union

**Ann-Sofie Ronnlund
Policy Officer
Trust and Security
Directorate General
Communications Networks, Content & Technology -
DG CONNECT
European Commission**



Towards a new ENISA mandate

- **Commission proposal 2010**
- **Political agreement Council/Member States and European Parliament – 29.1.2013**
- **Content and novelties**
 - ❖ **Duration (7 years)**
 - ❖ **Tasks (early warning, CERTs, international)**
 - ❖ **Governance (Executive Board)**
 - ❖ **Location (branch office in Athens)**
- **Final adoption in process**





Cybersecurity *The need for further EU action*

- **Economic and social benefits of the Digital Single Market**
- **Risks and incidents on the rise → Lack of trust, economic losses, missed opportunities**
- **Cross-border nature of risks and incidents**
- **Insufficient national preparedness and cooperation across the EU**





EU Cybersecurity Strategy *Objective and priorities*

"To ensure a safe and resilient digital environment in respect of fundamental rights and EU core values"

- **Strengthen security and resilience of networks and information systems**
- **Prevent and fight cybercrime**
- **A more coherent external EU cybersecurity policy**





Strengthen security and resilience of networks and information systems

- **Legislative measure**
 - ❖ **Directive proposal on Network and Information Security (NIS)**
- **Other measures**
 - ❖ **Fighting botnets; Security and resilience of Industrial Control Systems and Smart grids**
 - ❖ **Awareness raising; Training**
 - ❖ **Promoting Public-Private Partnership approach**
 - ❖ **Developing industrial and technological resources**
 - **Single market for cybersecurity solutions**
 - **Standards and public procurement**
 - **Foster R&D investments**





Prevent and fight cybercrime

- **European Cybercrime Centre**
 - ❖ **Programme Board (ENISA, EUROJUST, etc)**
- **Support to enhance national capabilities to investigate and combat cybercrime**
- **Encourage swift implementation of Cybercrime directives**





A more coherent EU external cybersecurity policy

- **Develop cyberdefence policy**
 - ❖ **Capability development (detection, response, recovery)**
 - ❖ **Synergies and dialogue between civilian and military players**
- **International cyberspace policy**
 - ❖ **Human rights and EU core values**
 - ❖ **Norms of behaviour**
 - ❖ **Capacity building in third countries**



Legislative proposal on NIS – Internal Market (Article 114 TFEU)

PREPAREDNESS
National capabilities

**EU-LEVEL
COOPERATION**
*comparable
capabilities and
mutual trust*



***A high level of NIS and
smooth functioning of
the internal market***

A CULTURE OF NIS ACROSS SECTORS
NIS risk management and Public-Private cooperation



Directive proposal on Network and Information Security (NIS) – *Key elements (1/3)*

- **Common NIS requirements at national level**
 - ❖ **National NIS strategy and NIS cooperation plan**
 - ❖ **National NIS competent authority**
 - ❖ **National/Governmental CERT with minimum capabilities**
 - ❖ **NIS exercises at national level**





Legislative proposal on Network and Information Security (NIS) – *Key elements (2/3)*

- **NIS competent authorities to cooperate within a network at EU level – NIS cooperation plan**
 - ❖ **Early warnings and coordinated response**
 - ❖ **Capacity building and peer reviews**
 - ❖ **NIS exercises at EU level**





Directive proposal on Network and Information Security (NIS) – *Key elements (3/3)*

- **Risk management**
- **Reporting of significant incidents**

for players in:

- ❖ **Energy – electricity, gas and oil**
- ❖ **Credit institutions and stock exchanges**
- ❖ **Transport – air, maritime, rail**
- ❖ **Healthcare**
- ❖ **Enablers of key Internet services**
- ❖ **Public administrations**





Role of ENISA ***EU Cybersecurity Strategy***

- **Provide expertise and advice**
- **Facilitate Public-Private dialogue**
- **Exercises: EU and international**
- **Awareness raising: EU and internationally**
- **Technical guidelines and recommendations**





Role of ENISA ***NIS Directive***

- **Provide expertise and advice: building and assessing national capabilities**
- **Assist the NIS cooperation network (consisting of national competent authorities for NIS)**
- **Practical guidelines; reporting templates**





European
Commission

Thanks!





Links

- **Digital Agenda for Europe: Trust & Security**
<http://ec.europa.eu/digital-agenda/en/telecoms-internet/trust-security>

