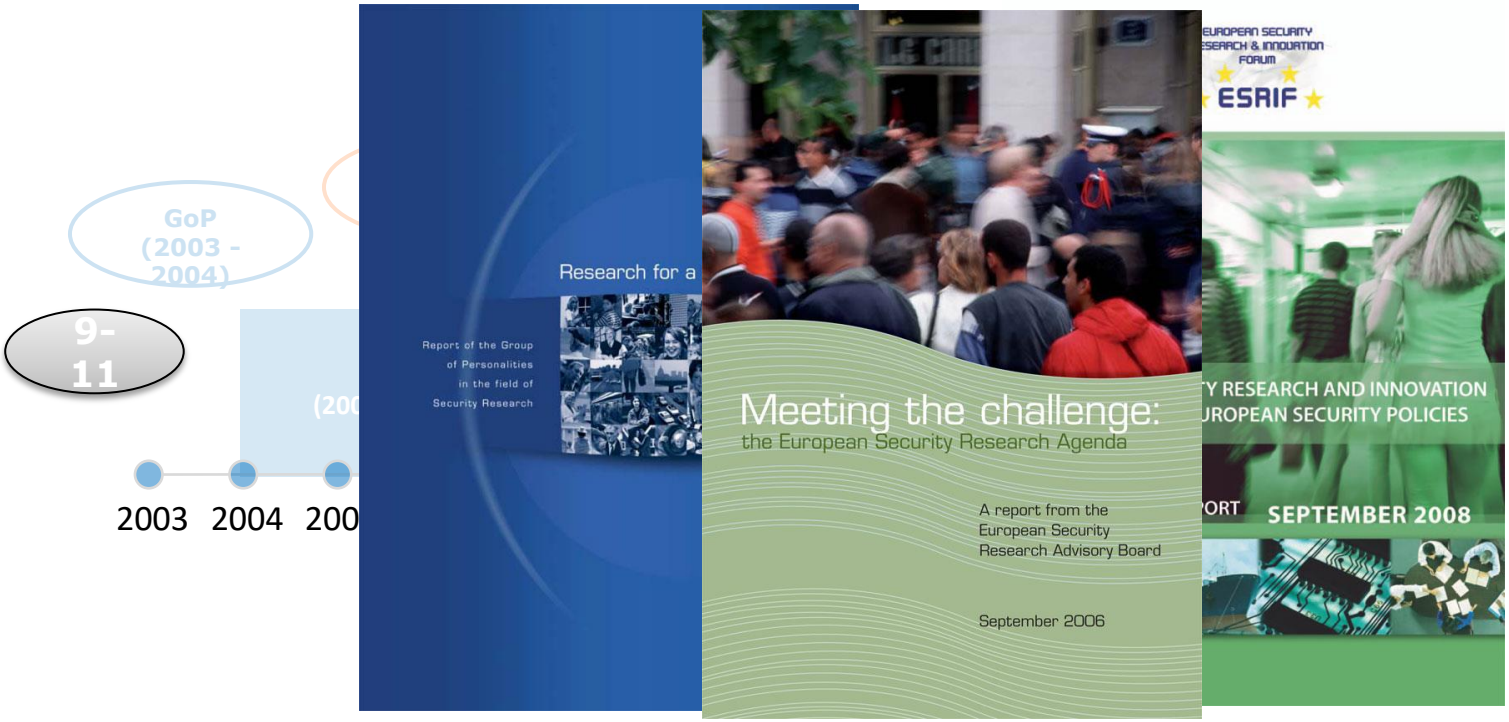
Particularities of Horizon 2020-Security

Infoday and brokerage event Riga, 9 April 2019

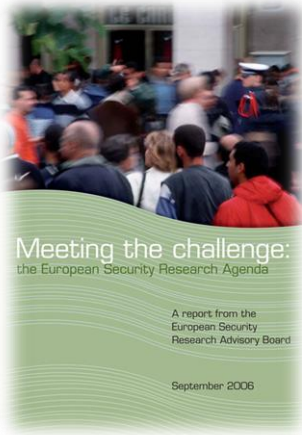
Armand Nachef (CEA)

History and rationale of the European Security research



Co-funded by the Horizon 2020
Framework Programme of the European Union

ESRAB recommandations



- **Follows a <u>mission-oriented</u> approach** *(initially 4 missions)*
- **Strengthens the involvement of the end-users in project definition and execution**
  - bring together at European level the 'demand' and 'supply' sides
- **Reinforces the role of the Member States' authorities (programme committee)**
- **Takes more into account the Societal Dimension**
  - Respect of privacy and civil liberties
- **Builds <u>Multidisciplinary projects</u>**
  - Integration of technological research and development with research into political, social and human sciences
- **Supports the EU industry to be competitive**
- **Ensures closer coordination with the activities of the European Defence Agency (EDA) to avoid unnecessary duplication**
- **Strengthens coordination with EU-Agencies: e.g. FRONTEX, EUROPOL, ENISA, EMSA, EU-LISA**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Figure

Border security

– overview diagram of the main functions, capabilities and technologies

Co-funded by the Horizon 2020
Framework Programme of the European Union

Figure 4

Protection against terrorism and organised crime

– overview diagram of the main functions, capabilities and technologies

Co-funded by the Horizon 2020
Framework Programme of the European Union

Figure 5

Critical infrastructure protection

– overview diagram of the main functions, capabilities and technologies

Co-funded by the Horizon 2020
Framework Programme of the European Union

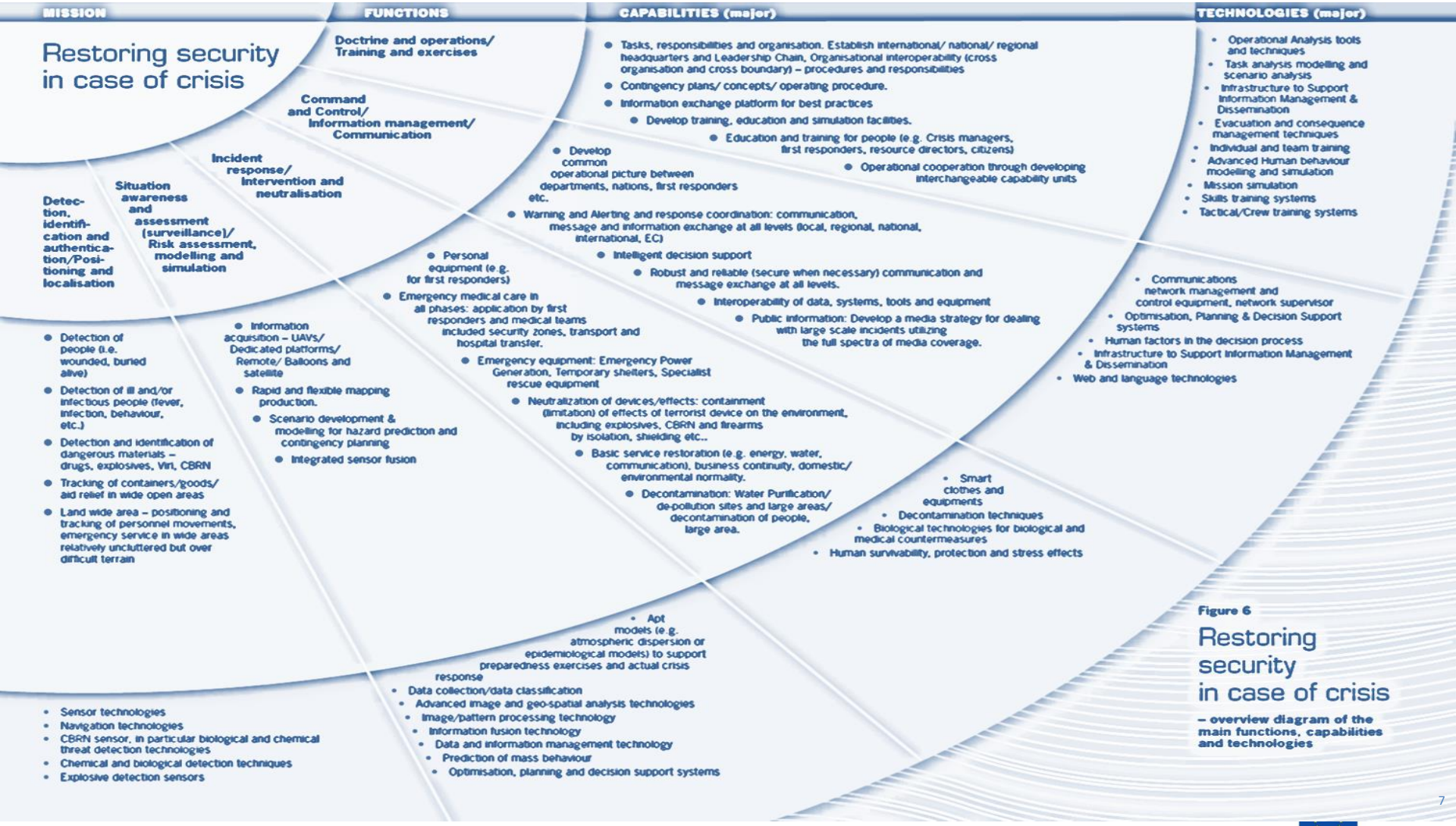


Figure 6

Restoring security in case of crisis

– overview diagram of the main functions, capabilities and technologies

Co-funded by the Horizon 2020
Framework Programme of the European Union

8 missions for Horizon 2020 - Security

1. Increase Europe's resilience to crises and disasters (SU-DRS) — DG Home
2. Protect and improve the resilience of critical infrastructures, supply chains and transport modes (SU-INFRA or CIP) — DG Home, DG CONNECT
3. Fight crime, illegal trafficking and terrorism, including understanding and tackling terrorist ideas and beliefs (SU-FCT) — DG Home
4. Strengthen security through border management (SU-BES) — DG Home
5. Support the Union's external security policies including through conflict prevention and peace-building (SU-BES) — DG Home
6. Improve cyber security (SU-DS and SU-ICT) — DG CONNECT
7. Ensure privacy and freedom, including in the Internet, and enhance the societal legal and ethical understanding of all areas of security, risk and management (SU-DS) — DG CONNECT
8. Enhance standardisation and interoperability of systems, including for emergency purposes — ALL

Co-funded by the Horizon 2020
Framework Programme of the European Union

WP Features 2019-2020:
The participation of practitioners (or other categories of participants) is a mandatory criterion in SEC and INFRA

Meaning of practitioners:

"A practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection."

- Applicants **have to identify which members of the consortium are "practitioners" in the specific context**
- Proposal template with specific table in template under Part B 4.3 (SEC and INFRA)

Co-funded by the Horizon 2020
Framework Programme of the European Union

WP Features 2019-2020:

Additional eligibility and admissibility conditions

An example:

This topic requires the active involvement of at least 3 first responders' organisations or agencies from at least 3 different EU or Associated countries (SU-DRS01-2019-2019-2020)

- these entities **have to be participants** and
- should be **directly involved** in carrying out the **tasks** foreseen in the grant.

- **2018: 15 proposals declared ineligible as not fulfilling the additional admissibility and eligibility conditions !!**

Co-funded by the Horizon 2020
Framework Programme of the European Union

WP Features 2019-2020:

Cross-cutting issues

- **Social Sciences and Humanities (SSH)** are integrated across all Horizon 2020 activities to successfully address European challenges

- **Gender dimension in the content of R&I** - a question on the relevance of sex/gender analysis is included in proposal templates

- The new strategic approach to **international cooperation** consists of a general opening of the WP and targeted activities across all relevant Horizon 2020 parts

Co-funded by the Horizon 2020
Framework Programme of the European Union

Appendix

POLITICAL REASONING BEHIND THE 2019 CALLS

Co-funded by the Horizon 2020
Framework Programme of the European Union

Political background to Horizon 2020

The Treaties

- The Eu Coal and Steel Community in 1951
- The Eu Atomic Energy Community in 1957
- … the single act in 1986 in EEC treaty for research policy
- The Lisbon Treaty 2007: Article 179 - ERA

The European Union institutions prepare Policies

- Research and Innovation Policy
- Regional Policy
- Education Policy
- …

Funding

- Horizon 2020
- European Structural and Investment Funds
- Erasmus Plus
- …

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA

Protecting the infrastructure of Europe and the people in the European smart cities

Protecting the Infrastructure

Co-funded by the Horizon 2020
Framework Programme of the European Union

The reasoning behind the INFRA call

- Threats against crowded areas and disruptions in the operation of our countries' infrastructure.
- Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.
- Recent terrorist attacks have shown a focus on so-called soft targets, which may have less long-term physical impact but which may be highly damaging in terms of victims and subsequent psychological and sociological impacts.

European Commission

Policy context - CIP

- CIP Policy:
  - Directive 2008/114/EC – Identification and designation of EU CI (Evaluation ongoing)
  - European Programme for CI Protection (COM (2006) 786, COM(2013) 318)
- Main priorities on CIP
  - Identification of tools, including indicators, to protect CIs from Hybrid Threats;
  - Methods and tools for addressing insider threats to CI, such as background checks and awareness raising in cooperation with relevant authorities;
  - New challenges to CIP and emerging threats (e.g. drones…)
  - Other: CI Risk assessment methods, transnational cooperation, civ-mil cooperation / cooperation with international orgs.

European Commission

Policy context - Protection Public Spaces

- **COM(2017) 612 – Action Plan protection of public spaces**
  - Guidance material and Exchange of best practices to support MS.
  - Improving cooperation between local actors and the private sector
  - Increased financial support: €18.5 million from the ISF. Further €100 million from the Urban Innovative Actions.
- COM(2018) 845 final - SU Progress Report, Dec. 2018 – State of play
- Main priorities on Protection of Public Spaces
  - Focus on known threats but also on emerging threats (e.g. drones, CBRN attacks)
  - Enhance cooperation between public actors, private actors and citizens.
  - New solutions to protect EU cities while maintaining their openness and not creating new vulnerabilities.
  - Consider the human factor.
- SRE 2018 Panel on Protection of Public Spaces
  - Take a look at the conference proceedings!!

European Commission

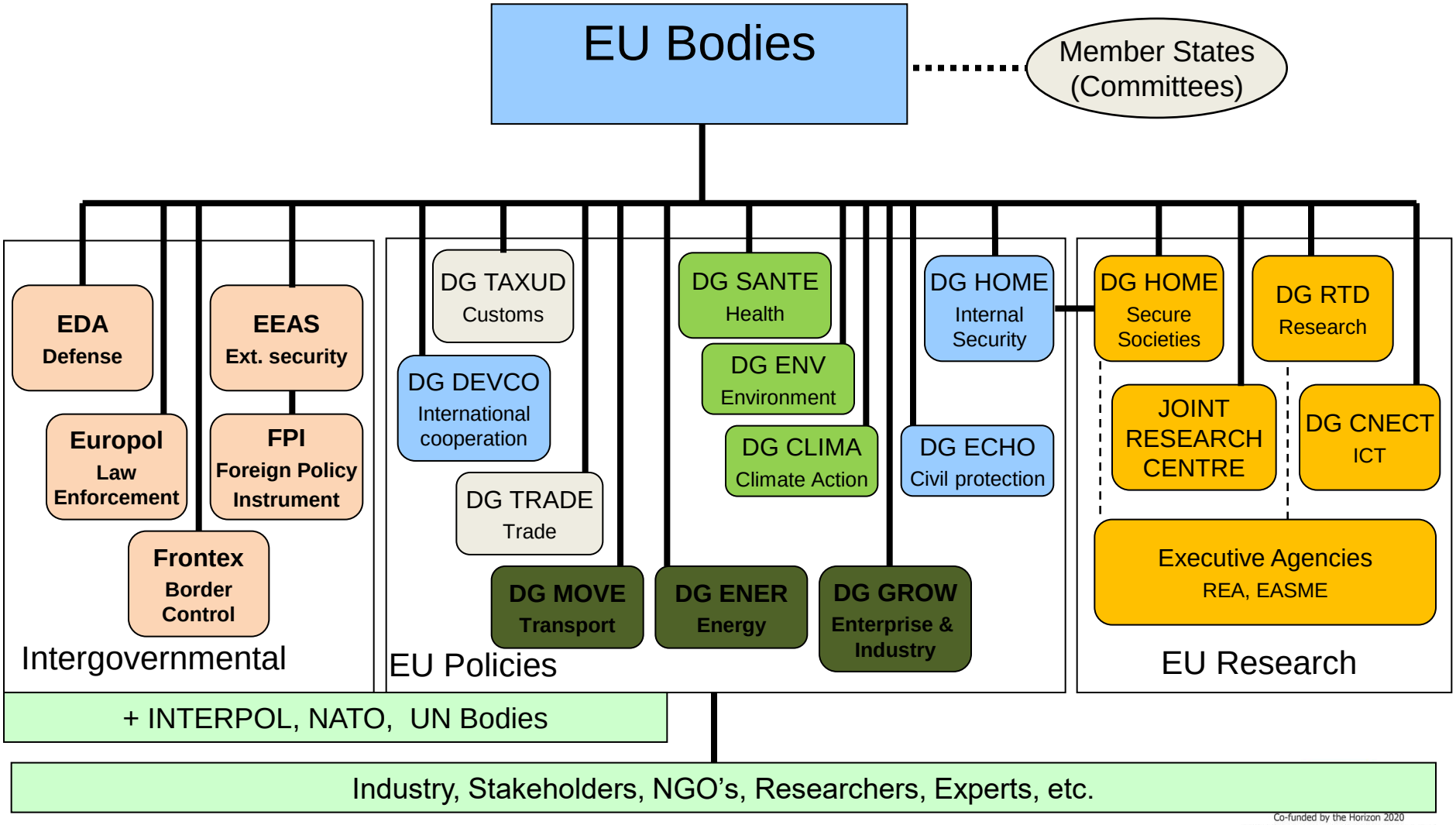
SU-DRS

Disaster-Resilient Societies

Resilience

Co-funded by the Horizon 2020
Framework Programme of the European Union

Disaster Resilient Societies - A complex policy landscape



Co-funded by the Horizon 2020 Framework Programme of the European Union

EU Policy context

Disaster Resilient Society

DG HOME
Internal Security

COM(2009) 273 final
CBRN Action Plan
+ COM(2014)247 final
CBRN-E risks
+ European Agenda on Security

DG ECHO
Civil Protection

Decision 1313/2013
EU Civil Protection Mechanism

Environmental threats

DG ENV
Environment

Decision 1386/2013
Environment Action Programme
Directives: Seveso III, Water Framework, Floods

Climate threats

DG CLIMA
Climate action

EU Climate Adaptation Strategy

Health threats

DG SANTE
Consumer Health

Decision 1082/2013
Serious cross-border threats to health

DG ENER
Energy

Regulation 347/2013
Tran-European Energy Instrastructure
Directive 2009/7/EU
Safety of nuclear installations

DG MOVE
Transport

Decision 661/2010
Tran-European Transport Network

DG TAXUD
Customs

EU Custom policy for supply chain security and use of customs detection technology for CBRN-E

International

DG DEVCO
International cooperation

CBRN-E Centres of Excellence

EEAS
Ext. security

Intergovernmental

+ UN Bodies, NATO

Nuclear non-proliferation treaty
Chemical Weapons Convention
Biological Weapons Convention

DG GROW
Enterprise & Industry

Security Industrial policy
COM(2012)417 final
Internal Security Strategy
COM(2010)673 final
European Agenda on Security

DG TRADE

Regulation 428/2009
Transit of dual use items

HORIZON
2020

EU Reseach

EDA
Defense

Joint Investment Programme / EFC

Co-funded by the Horizon 2020 Framework Programme of the European Union

SU-FCT

Fight Against Crime and Terrorism

Fight against Crime

Fight against Terrorism

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context

The European Agenda on Security defines the priority actions at EU level to ensure an effective EU response to security threats over the period 2015-2020:

*(…)"**Terrorism, organised crime and cybercrime** are the three core priorities which are highlighted in this Agenda for immediate action. They are clearly interlinked and cross-border threats, and their multi-faceted and international dimension shows the need for an effective and coordinated response at EU level". (…)*

(…)"The response to cybercrime (e.g. phishing) must involve the entire chain: from Europol's European Cybercrime Centre, Computer Emergency Response Teams in the Member States concerned by the attack, to internet service providers that can warn end-users and provide technical protection. In short, cybercrime demands a new approach to law enforcement in the digital age." (…)

Co-funded by the Horizon 2020
Framework Programme of the European Union

The 9th Security Union progress report

- Based on a comprehensive assessment of EU security policy since 2001, the report highlights the remaining gaps and challenges to be addressed. **Incomplete implementation of existing policies remains a challenge, as do evolving threats such as radicalisation and cybercrime — which may require changes to existing instruments.**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context - forensics

- 06/2016: Council Conclusions on the way forward in view of the creation of a European Forensic Science Area
  - a detailed action plan with six specific areas:
    - Best Practice Manuals for forensic disciplines.
    - Stimulating exchange of forensic information from databases, for example in the area of weapons and ammunition, explosives and drugs.
    - Proficiency tests and collaborative exercises for forensic disciplines.
    - Forensic awareness and training for law enforcement and justice communities.
    - Stimulating accreditation of forensic service providers and competence of forensic personnel on a voluntary basis.
    - Stimulating exchange of forensic data via Prüm and improving quality.

  - the Council noted that additional funding from the European Commission would be crucial for implementing the new action plan and developing the European Forensic Science Area, calling for support for forensic sciences via Horizon 2020 and Internal Security Funds

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context - cybercrime

- **09/2017:** Cybersecurity package (COM(2017)477**)**

- **A more effective law enforcement response focusing on detection, traceability and the prosecution of cyber criminals is central to building** an effective disincentive to commit such crimes. The Commission is therefore proposing to boost deterrence through new measures to combat fraud and the counterfeiting of non-cash means of payment.

- The proposed Directive will strengthen the ability of law enforcement authorities to tackle this form of crime by expanding the scope of the offences related to information systems to all payment transactions, including transactions through virtual currencies. The law will also introduce common rules on the level of penalties and clarify the scope of Member States' jurisdiction in such offences.

- Background: Recent figures show that digital threats are evolving fast and that the public perceives cyber-crime as an important threat: Whilst ransomware attacks have increased by 300% since 2015, the economic impact of cyber-crime rose fivefold from 2013 to 2017, and could further rise by a factor of four by 2019, studies suggests. **87% of Europeans regard cybercrime as an important challenge to the EU's internal security.**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context – child sexual abuse and exploitation

- (12/2016) the Commission adopted two reports on the measures taken by MSs to combat the sexual abuse and sexual exploitation of children and child pornography:
    - one report covers the entire Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011/92/EU);
    - the other report focuses on the measures against websites containing or disseminating child pornography.

- The reports present a first overview of measures taken by Member States to transpose the Directive into national law. The reports show that, although the Directive has led to substantial progress, there is still considerable room for improvement, in particular with regard to **prevention and intervention programmes for offenders, the assistance, support and protection measures for child victims**, **the prompt removal of child sexual abuse material in Member States' territory** and the provision of adequate safeguards when the optional blocking measures are applied.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context: anti-terrorism, “soft targets” & abuse of encryption

- The 11th Security Union progress report (102017): Commission presented **anti-terrorism package** to better protect EU citizens - a package of operational and practical anti-terrorism measures to be rolled out over the next 16 months. These measures will help MSs address vulnerabilities exposed by recent terrorist attacks and will make a real difference in enhancing security. The measures will, amongst other:
- Support Member States in protecting public spaces (and so-called *"soft target" protection*);
- Close the space in which terrorists can operate by further restricting access to explosive precursors and improving cross border access to financial information;
- *Support law enforcement and judicial authorities that encounter encryption by criminals in criminal investigations;*
- Set out the next steps on countering radicalisation;
- Reinforce the EU's external action on counter-terrorism.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES

Border and External Security

Co-funded by the Horizon 2020
Framework Programme of the European Union

The reasoning behind the BES call

Development of technologies, capabilities and solutions to:

- Improve EU border security:
  - Flow of people: research will support the exploitation of the potential given by the **European Border Surveillance System** (EUROSUR - Regulation No 1052/2013) and promote an enhanced use of new technology for border checks in relation to the **SMART BORDERS** legislative initiative (DG HOME)
  - Flow of goods: research will address, in the context of the EU's customs policy, supply chain security trying to strike the right balance with trade facilitation (DG TAXUD)
- Support the EU External Security Policies in civilian tasks (EEAS).

.. But also <u>understanding the phenomena</u> with impact on border and external security. Social sciences and humanities involved.

Co-funded by the Horizon 2020
Framework Programme of the European Union

The Policy landscape

EU Agenda on Security

Organised Crime & Human Trafficking

We help EU States in taking consistent action to effectively prevent and counter the many facets of modern organised crime.

- THB Directive
- Expl. of Children Directive
- Serious and Organised Crime

EU Agenda on Migration

Schengen, Borders & Visas

The EU's common external border calls for EU States' cooperation on border control and visa policy to ensure freedom and security within Europe.

- Smart Borders
- Document fraud

Irregular Migration & Return

In 2014, 276 113 migrants entered the EU irregularly via land, air and sea routes. Most migrants have recourse to criminal networks of smugglers.

- EUROSUR
- Migrant Smugg.

- Interoperability of EU Information systems
- European Border And Coast Guard

Taxation and Customs Union

- EU Customs Strategy
- Union Customs Code

Union External Security Policies in Civilian Tasks

- CSDP

*COM(2018) 845 final - SU Progress Report, Dec. 2018 – State of play

Co-funded by the Horizon 2020 Framework Programme of the European Union

SU-GM

General Matters

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy Context

04/2015: **European Agenda on Security** defines the priority actions at EU level to ensure an effective EU response to security threats over the period 2015-2020

"**Research and innovation** is essential if the EU is to keep up-to-date with evolving security needs. Research can identify new security threats and their impacts on European societies. It also contributes to creating social trust in research-based new security policies and tools. Innovative solutions will **help to mitigate security risks** more effectively by drawing on **knowledge**, research and **technology**."

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy Context

10/2016: new Commissioner for the Security Union, supported by a horizontal Task Force involving 30 different services in the Commission and the EEAS

Mission letter of Julian King as Commissioner for Security Union:

"During our mandate, I would like you to support the Commissioner for Migration, Home Affairs and Citizenship in the following tasks:

[…] "Ensuring that EU-financed security research targets the needs of security practitioners and develops solutions to forthcoming security challenges […]."

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy Context

12/2018 Seventeenth Progress Report towards an effective and genuine Security Union

Section on EU Security Research

'EU security research is one of the building blocks of the Security Union enabling innovation in technologies and knowledge crucial for developing capabilities to address today's security challenges, anticipating tomorrow's threats and contributing to a more competitive European security industry.'

'Given the particular nature of the security sector (in which the market is represented mainly by public authorities), **appropriate uptake of research output can be guaranteed only if research is acknowledged as one of the building blocks of a wider capability development process bringing together policy-makers, practitioners, industry and academia. The close involvement of all stakeholders at an early stage is instrumental to identify capability gaps, and define capability priorities that can, when needed, trigger research requirements.'**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Evolving threat landscape in cybersecurity

- Proliferation of (poorly secured) IoT devices
- Blurring lines between state and non-state actors
- Hybrid attacks on western democracies
- Fake news
- Evolving cybercrime business models
- Cyber espionage on the rise
- Dependence on foreign security technologies
- Persisting critical infrastructure vulnerabilities
- Attempts to promote new internet governance model
- Vulnerabilities of third countries

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context (1/5)

- **Digital Single Market Strategy – COM(2015) 192;**

- **European Agenda for Security – COM(2015) 185;**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context (2/5)

- **NIS Directive – Directive (EU) 2016/1148 of 6/7/2016 concerning measures for a high common level of security of network and information systems across the Union;**

- **eIDAS – Regulation (EU) 910/2016 of 23.7.2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;**

- **General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;**

- **Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" – COM(2016) 410 of 5.7.2016;**

- **Contractual Public-Private Partnership on Cybersecurity – July 2016;**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context (3/5)

Proposal for an e-Privacy regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - COM(2017) 10 of 10.1.2017;

State of the Union 2017 - speech of the President of the Commission (13/09/2017)

- ✓ **cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks;**
- ✓ **there is a need for a Europe that protects, empowers and defends;**
- ✓ **the priority is to better protect Europe in the digital age;**

Cybersecurity Package 2017 (13/09/2017)

- ✓ **Joint Communication JOIN(2017)450: The Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.**

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context (4/5)

Conclusions from the Tallinn Digital Summit (29/09/2017):

- "We should make Europe a leader in cybersecurity by 2025, in order to ensure the trust, confidence, and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet."

- "Europe needs a common European approach to cybersecurity. Europe has to function as a single European cyberspace and a single cybersecurity market, including in terms of world-class and state-of-the-art security certification and joint standards, operational capacity, and collective crisis response."

Co-funded by the Horizon 2020
Framework Programme of the European Union

Policy context (5/5)

Council Conclusions (20 November 2017)

… "21. WELCOMES the intention to set up a Network of Cybersecurity Competence Centres to stimulate the development and deployment of cybersecurity technologies and to offer an additional impetus to innovation for the EU industry on the global scene in the development of next-generation and breakthrough technologies, such as artificial intelligence, quantum computing, blockchain and secure digital identities;

22. STRESSES the need for the Network of Cybersecurity Competence Centres to be inclusive towards all Member States and their existing centres of excellence and competence and pay special attention to complementarity and with this in mind NOTES the planned European Cybersecurity and Research Centre, which should, as its key role, focus on ensuring complementarity and avoiding duplication within the Network of Cybersecurity Competence Centres and with other EU agencies;" …

Co-funded by the Horizon 2020
Framework Programme of the European Union