

## Horizon Europe

- **What?** The future EU research and innovation programme
- **When?** 2021-2027
- **Timeline:** At the moment the Council and European Parliament are negotiating and subsequently adopting the programme. On 1 January 2021 Horizon Europe will be launched
- **Available budget:** €100 billion
- **More information:** [here](#)
- **Relevance for crime prevention activities:**

The new programme will be implemented through **three pillars**:



Pillar 2 **Global Challenges and European Industrial Competitiveness** (€52.7 billion) includes six broad thematic “clusters” of activities. Cluster 3 focuses on **civil security for society**. This cluster has as its vision to **support wider EU responses to security challenges** i.e. to support ‘a resilient and more stable Europe that protects’ as well as for this purpose supporting a competitive European civil security industry sector. It will address the challenges arising from persistent security threats like terrorism and crime, including cybercrime, as well as natural and man-made disasters.

### EU policy objectives

As regards protection and security, R&I activities will support implementation of relevant EU policies including those developed under the framework of the **European Agenda on**

**Security** and the **development of a Security Union**. These include policies on integrated border management, the EU Action Plan on the protection of public spaces, policies and instruments on protecting critical infrastructure, as well as on fighting crime, including cybercrime and terrorism.

**Cybersecurity**, as addressed by the digital and privacy policy of the Union, in particular the NIS Directive, the GDPR, the EU Cybersecurity Act, and the future e-Privacy Regulation will benefit from R&I activities so as to keep up with rapid technological developments and the understanding of emerging trends in the cyber-domain.

As an overarching priority, effective support will be provided to practitioners, law enforcement agencies, first responders and other public authorities or private entities which are ensuring the security of European citizens, infrastructures and assets in general.

### **Targeted impacts**

The main impacts sought are to support implementation of EU policy priorities relating to security, including cybersecurity, and disaster risk management

- **improved disaster risk management and societal resilience**, leading to reduced losses from man-made and natural disasters;
- **improved management of air, land and sea EU external borders**, leading to better monitoring of movements across external borders and reduction of illegal movements of people and goods across those borders;
- **better protection of citizens from violent attacks in public spaces**, through more effective prevention, preparedness and response while preserving the open nature of such spaces;
- **improved security and resilience of infrastructure and vital societal functions**, so as to minimise disruptions
- **improved maritime security**, including from man-made and natural disasters and from security challenges such as trafficking, piracy and potential terrorist attacks, cyber and hybrid threats, notably through better maritime surveillance and capability development;
- **fighting crime and terrorism more effectively**, particularly through better prevention of criminal acts and enhanced investigation capabilities notably as concerns cybercrime;
- **cybersecurity and a secure online environment**, with citizens, public bodies and companies empowered to protect their data and online activities.