eucrim
European Law Forum: Prevention • Investigation • Prosecution

Security – A Firm Construct or an Undetermined Concept?

An Outline of the EU's Current and Future Security Architecture

Elisa Sason, Cristina Monti, Pablo Olivares-Martinez [*]

ABSTRACT

The concept of security within the EU's legislative and policy framework has evolved significantly over the past few decades, adapting to shifting realities. Building on existing and overarching foundations, notably the EU Security Union Strategy, the European Commission recently presented a trio of initiatives that further frame the EU's approach towards security. Having begun with a focus on conventional threats, such as terrorism and organised crime, the EU's security approach has expanded to encompass cyberattacks, hybrid threats, and the protection of critical infrastructure.
This article gives an overview of the most prominent adopted initiatives that have shaped, shape and will shape the EU's security architecture. The authors argue that the concept of security can no longer be viewed in isolation and that it should be seen as intersecting with a wide range of different instruments, actions, and policy areas. The authors consider it essential to establish clarity regarding the EU's concept of security as well as its governance structures in order to develop an efficient approach towards tackling existing and future threats. Continuous attention and vigilance will need to be paid to ensure a coordinated and horizontal approach to protect EU security.

AUTHORS

Elisa Sason
Policy Coordinator
European Commission

Cristina Monti
Policy Coordinator
European Commission

Pablo Olivares-Martinez
Policy Coordinator
European Commission

CITE THIS ARTICLE

Monti, C., Olivares-Martinez, P., & Sason, E. (2025). Security – A Firm Construct or an Undetermined Concept? An Outline of the EU's Current and Future Security Architecture. Eucrim – European Law Forum: Prevention • Investigation • Prosecution. https://doi.org/10.30709/eucrim-2025-004

Published in eucrim 2025, Vol. 20(1) pp 43 – 52

https://eucrim.eu

ISSN: 1862-6947

I. Introduction

While the concept of security has always been high on the European Union's political agenda, it has become increasingly prominent in recent years. Different wars and crises, as well as rapidly evolving global events continue to unfold daily. The challenges to security and stability on the European continent are greater than at any time since World War II, and the need for clarity on the concept of security is particularly crucial now.

But what is security? And what should it mean for citizens to feel secure in the EU? According to the EU's Treaty on the European Union (TEU), the values of respect for human dignity, freedom, democracy, equality, the rule of law, and respect for human rights are the fundamental principles of the Union, with the ultimate goal of promoting these values and the well-being of its people – especially peace.[1]Taken with the Treaty on the Functioning of the European Union (TFEU), this underpins the Union's overarching objective of providing citizens with a high level of protection in the areas of freedom, security and justice.[2] At the same time, it is clear from the Treaties that national security is a sole responsibility of each Member State[3] and that separate rules apply for the development of the Union's common foreign and security policy. Furthermore, while the Treaties provide a good starting point, they do not offer a definition of the concept of security that could apply across the Union and its legislation and policies. As we will see, this is a significant deficiency, particularly at a time when security challenges are fast growing.

Based on the rules in the core treaties, the Union has adopted a tremendous amount of legislative and policy initiatives over the past several decades, with the goal of creating and strengthening the EU's area of freedom, security and justice. These rules provide common standards across the Union to combat serious crime, improve cooperation between police and judicial authorities, and enhance the Union's overall resilience against different types of attacks. While the traditional focus of the Union's actions in the area of security have focused on preventing terrorist attacks, protecting borders, and fighting organised crime, now shifting geopolitical interests and emerging new technologies demonstrate the need to apply a broader horizontal approach towards security. Providing citizens with security based on a comprehensive and enforceable framework is an endeavour requiring heightened attention to considerations far beyond the conventional justice and home affairs agenda. This means first recognising the inextricable links between the Union's external security and security within its own borders but also expanding our working understanding of the security concept to areas such as the economy, energy, digitalisation, public health, transport, and climate, and addressing them effectively in defence policy.

This article outlines initiatives taken by the EU to protect its security, notably under the umbrella of the EU's Security Union Strategy 2020-2025 (section II) and explains recently adopted initiatives in this area as announced by the Political Guidelines for the new European Commission 2024-2029 (section III). It also presents the views from other EU Institutions and actors in the area of security (section IV), before concluding with a number of final considerations (section V).

II. An Evolving EU Security Policy: From Internal Priorities to a Comprehensive and Silo-breaking Approach

Over the past decades, the evolution of the EU's security policy has paralleled the changing global threat landscape and the Union's commitment to safeguarding its citizens and core values. This is one of the youngest policy areas at the EU level, stemming from a gradual transition from informal collaboration among an expanding number of Member States to inter-governmental cooperation and then to further integration based on common laws and initiatives. The first EU internal security strategy, covering 2010-2015,[4] primarily focused on traditional internal security priorities, such as organised crime and terrorism; however, it also included natural and man-made disasters. This foundational phase provided the necessary coordination among EU Member States's push to tackle cross-border and cross-sectoral threats to which no single Member State could effectively respond on its own.

A series of high-profile terrorist attacks in subsequent years prompted a significant strategic shift in Member States' approach towards security. The European Agenda on Security 2015-2020,[5] under the guidance of Commissioner *Julian King*, emerged as a response to these threats and demonstrated the need for greater cooperation between national authorities, EU institutions, and various stakeholders, including the private sector. This agenda went beyond a conventional approach to security threats, paving the way for a Security Union concept. It marked a transition from the traditional focus on internal vulnerabilities to the recognition that modern security challenges are increasingly transnational and multifaceted.

The advent of the **Security Union Strategy 2020–2025**,[6] entrusted to Commission Vice-President *Margaritis Schinas*, took this shift further. This strategy was designed at the peak of the COVID-19 pandemic, and it was founded on four strategic pillars: (i) creating a future-proof security environment, ii) tackling evolving threats, iii) protecting Europe from terrorism and organised crime, and iv) building a robust European security ecosystem. The Strategy aimed to provide a holistic and comprehensive approach to security in an increasingly complex threat landscape marked by hybrid threats, disinformation, and increasing geopolitical volatility – with unprecedented challenges to EU values and democracies. It targeted areas where the EU could bring added value to national efforts and placed a particular emphasis on cybersecurity, the protection of critical infrastructure, hybrid threats, and the nexus between internal and external security.

During its timespan, new initiatives were incorporated under the umbrella of the Security Union Strategy in response to a number of specific circumstances that could not have been foreseen when it was first designed. It was not only the Russian war of aggression against Ukraine and the deteriorating situation in the Middle East that required additional and more decisive actions but also rapid technological developments. This was true, in particular, for the newer areas of focus in the original Strategy (critical infrastructure, cybersecurity, and hybrid threats), and they have been intensified in response to severe events. Examples of these new initiatives include the Cyber Solidarity Act,[7] the anti-corruption package,[8] and measures to counter migrant smuggling.[9] Parallel to the overarching framework provided by the Security Union Strategy, the Commission adopted targeted strategies in key security domains, including counterterrorism,[10] organised crime,[11] drug trafficking,[12] and trafficking in human beings.[13] This multi-pronged approach reflects the understanding that modern security challenges are interlinked and that vulnerabilities in one area can have cascading effects on others. An example illustrating an integrated approach where physical and cyber threats are addressed in tandem is the measures taken to protect public spaces and entities providing essential services, which have been coupled with efforts to secure digital infrastructures.

Over 40 legislative initiatives under the umbrella of the Security Union Strategy were proposed by the Commission and successfully adopted by the co-legislators (European Parliament and Council) in 2020-2025.[14] Key legislative achievements concern the protection and enhancing of the resilience of critical infrastructure in the EU against physical and digital threats, with the parallel adoption of the Directives on Critical Entities Resilience (CER)[15] and Network and Information Systems (NIS2).[16] Together, and once fully transposed and implemented by Member States, these Directives will ensure that risks and vulnerabilities affecting entities in a range of key sectors, such as energy, transport, and space, are better addressed. With the adoption of the Cyber Resilience Act[17] and the Cyber Solidarity Act,[18] the EU has been a pioneer in creating a solid legal framework to reinforce the cybersecurity of products with digital elements and supply chains, to strengthen solidarity at the EU level in case of major cyber incidents, and to enhance its collective capabilities to detect, prepare for, and respond to these types of risks.

At the same time, more "typical" security areas, such as the fight against organised and serious crime, continued to receive attention under the Security Union Strategy, with pivotal legislation adopted to tackle cybercrime (notably the e-evidence package[19]), trafficking in human beings,[20] and environmental crime[21] as well as money laundering and terrorism financing.[22] The new rules on asset recovery and confiscation[23] should lead to higher rates of confiscation of criminal proceeds – currently stagnating at an estimated 2% of illicit proceeds[24] – and allow for a stronger focus on crypto assets. A related area of major importance to the Strategy concerned the improvement of cooperation between police authorities and their operational capabilities. No less than three initiatives branded as the "EU Police Cooperation Code" were adopted: the Regulation on Automated Data Exchange for Police Cooperation (Prüm II),[25] the Directive on information exchange between law enforcement authorities and Member States,[26] and a Council Recommendation on operational police cooperation.[27] Through timely and accurate implementation, these measures are expected to significantly step up law enforcement cooperation across Member States and grant police officers more modern tools by which to exchange information.

While advancing the work on the Security Union Strategy and following the return of war to the European continent, the **Strategic Compass**[28] of March 2022 presented an ambitious plan of action for strengthening the EU's security and defence policy. With the objective of boosting the EU's cyber defence capabilities, enhancing situational awareness, and coordinating the entire range of defensive options available, this Compass aimed for a heightened level of resilience, a better response to cyber-attacks, and enhanced solidarity as well as improved mutual assistance. Increasing emphasis has been put on improving the EU's capacities to counter hybrid threats. In addition to mechanisms, such as the Foreign Information Manipulation and Interference (FIMI) Toolbox and the Cyber Diplomacy Toolbox to be better prepared for and respond to cyberattacks, the EU put in place the Hybrid Toolbox, which is now operational and is used to respond to the intensified hybrid campaign by Russia targeting the EU and its Member States. Moreover, the idea of deploying EU Hybrid Rapid Response Teams was developed to offer short-term, tailored support to Member States and partner countries. Also noteworthy is the fact that the Strategic Compass identified space as a fifth operational domain of warfare (alongside land, sea, air, and cyber domains) and proposed measures to improve the collective protection of space systems and services against threats.[29]

Central to the Security Union Strategy has been its focus on **implementation**, with the Commission adopting seven progress reports to regularly report on progress achieved in the 2020-2024 period.[30] The final progress report[31] of the Strategy adopted in May 2024 concluded with an outlook on **security challenges beyond 2025**. Accessing data in cutting-edge technologies like quantum communication infrastructure, artificial intelligence, and advanced surveillance pose significant challenges, highlighting the need to continue exploring how law enforcement can make use of digital technologies, while also ensuring the full respect for fundamental rights and cybersecurity.[32] Indeed, the intersection of technology and security presents a growing paradox: we must protect data and technological advancements, in line with EU values and principles, yet these very assets can also be exploited by criminals for illicit activities.

The final progress report called for a fresh approach to the way EU institutions and bodies and Member States respond to challenges, guaranteeing the EU's capacity to respond swiftly when necessary as well as avoiding silos and response mechanisms that duplicate risk assessment or complicate crisis response.[33] Here, the challenge lies in translating this into practical action within an increasingly complex security ecosystem, where multiple players with overlapping goals and responsibilities must navigate a delicate balance. The Joint Cyber Unit, identified by the Security Union Strategy as a crucial mechanism for coordin-

https://doi.org/10.30709/eucrim-2025-004

ated and structured operational cooperation across the civilian, law enforcement, diplomatic, and defence communities serves as a prime example of how promising initiatives can lose momentum.

Finally, the progress report acknowledged that the Union's understanding of the notion of security has broadened, as the risks facing the EU have multiplied. The need for Europe to become more autonomous and less dependent on third countries (be it in the area of technology or in the provision of critical products and services) brings with it a range of economic considerations situated at the interface between security and competitiveness. The report further emphasised that any modern approach to security must integrate both digital and cyber components and take international implications into consideration, while also ensuring that security is embedded in all EU policies and decision-making processes.[34]

III. Current and Future Priorities

> Extraordinary times call for extraordinary measures. This is also true for my Commission. To deal with the challenging way ahead, we need to switch into a preparedness mind-set. This is why, in the next weeks, I will convene the first-ever Security College. This will ensure that the College members receive regular updates on security developments. From external and internal security to energy, defence and research. From cyber, to trade, to foreign interference. Only if we have a clear and in-depth understanding of the threats, including hybrid threats, can we effectively contribute to collective security.
>
> Ursula von der Leyen, 9 March 2025

Given the current geopolitical context, it comes as no surprise that the notion of security is predominant in the Political Guidelines of Commission President *Ursula von der Leyen* during her second term of office.[35] In the Chapter "A new era for European Defence and Security", she announced her vision for a new approach to crisis and security preparedness. Among the main initiatives listed in this section are the adoption of a Preparedness Union Strategy inspired by the 2024 Niinistö Report and a European Internal Security Strategy to ensure that security is integrated into EU legislation and policies by design. In line with this direction, President von der Leyen announced specific initiatives: to make Europol a truly operational police agency, to reflect on areas where the European Public Prosecutor's Office's (EPPO) mandate could be extended,[36] and to design a new EU action plan against drug trafficking, an EU Port Strategy with a strong focus on security, a new Counter-Terrorism Agenda, and a new European Critical Communication System – to be used by authorities in charge of ensuring security and safety.

The concept of the "Security College" was also announced by Commission President *von der Leyen* in a speech marking the first 100 days of her Commission's mandate.[37] It aims to anchor security in the Commission's policymaking, ensuring that the College of Commissioners receives regular updates on security developments in all policy areas.

The consolidation of security is also a red thread in the letters that Commission President von der Leyen sent to Commissioners-designate, setting their missions for this mandate.[38] First, Executive Vice-President *Henna Virkkunen* is responsible for the portfolio Tech Sovereignty, Security and Democracy, a title that implies a supervisory role in security policies, including internal security and defence. Furthermore, the Executive Vice-President is in charge of key security areas, such as cybersecurity. Second, Commissioner *Magnus Brunner* is responsible for Internal Affairs and Migration, focusing on the traditional aspects of security, such as the fight against terrorism and organised crime; he is also tasked with delivering on the Internal Security Strategy. Commissioner *Andrius Kubilius* is the first-ever appointed Commissioner for defence. Preparedness, a policy closely linked with security, is included in the remit of Vice-President *Roxana Mînzatu* and Commissioner *Hadja Lahbib*.

In her mission letters, Commission President *von der Leyen* calls on all Commissioners to draw on recent, high-profile reports addressing security policies. These include, in particular, the 2024 Draghi Report on the future of European competitiveness and the 2024 Niinistö Report on how to enhance Europe's civilian and defence preparedness and readiness. The main security-related aspects of these reports and the linked initiatives adopted in this mandate, are described in the following sub-sections.

Competitiveness as a prerequisite for securing prosperity and freedom

Presented on 9 September 2024, the Draghi Report on EU competitiveness[39] arrived at a crucial moment in the core mission of strengthening the Union's competitiveness. With 176 concrete recommendations made in a range of sectors, the report is built on three key anchors: i) closing the innovation gap with the United States and China, particularly in advanced technologies; ii) a joint action plan for decarbonisation and competitiveness; and iii) increasing security and reducing dependencies from third countries.[40] Cutting regulatory burdens, using collective spending power in crucial areas such as innovation and defence, and applying stronger horizontal EU coordination are means to achieve these goals. Together with Enrico Letta's 2024 Report on the Future of the Single Market,[41] Draghi's steer is seen as key not only to reinvigorating the EU's competitiveness but to safeguarding its economic security.

The European Commission responded with the adoption of **the Competitiveness Compass** on 29 January 2025,[42] setting out a roadmap with legislative and policy initiatives for the next five years to implement the recommendations of Draghi's report. Based on the three key anchors identified by Draghi, the Compass introduces *transformational imperatives* to boost the EU's productivity gap, particularly in the tech area, as a way to strengthen competitiveness. Preparedness and security are also part of the agenda; reference is made to new actions flowing from the joint White Paper on the future of European Defence, the Preparedness Union Strategy, and the Internal Security Strategy. Five enablers are guiding horizontal requirements for the implementation of the Compass across all policy sectors: i) simplifying the regulatory environment, ii) fully exploiting the potential of the EU's Single Market, iii) providing financing through a Savings and Investments Union as well as a refocused EU budget, iv) promoting professional skills and high-quality jobs and iv) improving policy coordination at the EU and national levels.

Preparedness as a mindset and standard course of action

On 30 October 2024, former Finnish President *Sauli Niinistö* presented his report on strengthening Europe's civilian and military preparedness and readiness.[43] Aimed at informing future actions to be proposed by the High Representative for Foreign Affairs and Security Policy (in the following: High Representative) and the Commission in view of the Political Guidelines and mission letters to Commissioner-designates, this report is a clear wake-up call to the EU on the need for action, and it sets out a number of specific steps. The actions proposed relate to cross-cutting areas of strategic importance which include – but are not limited to – the EU's military capabilities, the provision of healthcare and building up sufficient stockpiles, the secure use and development of digital technologies, and the availability of critical raw materials and components. The Niinistö Report confirms the important link between security and competitiveness, underscoring Europe's need to be economically competitive – not only to keep itself and its businesses secure but also to make a real impact on international developments instead of merely adjusting to them.[44]

The Niinistö Report also underlines the need for the EU to consider and concretely prepare for worst-case emergency and crisis scenarios and to take more strategic responsibility in a world subject to constant change. The idea is to follow an integrated *whole of EU society* method, bringing together relevant stakehold-

https://doi.org/10.30709/eucrim-2025-004

ers: national authorities, private entities, employers, trade unions, civil society organisations as well as – and perhaps most importantly – individual citizens. While the "whole of society" approach already made its appearance in the Security Union Strategy, its inclusion in future strategies remains relevant.

The ideas presented in the Niinistö Report were translated into the **European Preparedness Union Strategy,** adopted by the Commission and the High Representative on 26 March 2025.[45] The aim of this Strategy (accompanied by an action plan with 63 items and an indicative timeline for their implementation) is to establish a comprehensive framework ensuring the EU's preparedness to respond to any type of crisis, including climate change, health emergencies, natural disasters, and security infrastructure attacks. The Strategy is horizontal in nature, and it fosters a culture of preparedness and resilience, thereby supporting the obligation of Member States under Art. 222 TFEU to act in solidarity in the event of crises. The actions proposed revolve around seven areas[46], and include the development of an EU comprehensive risks and threats assessment. The latter will be done through the following: strengthening the Single Intelligence Analysis Capacity (SIAC); a future Climate Adaptation Plan; practical measures to increase preparedness of citizens to ensure self-sufficiency for a minimum of 72 hours; and the boosting of public-private cooperation and the EU-NATO partnership.

The Strategy also includes a section on ensuring the resilience of vital societal functions. Reference is made to the work carried out under the previous Commission mandate in the context of the Security Union as regards the protection of critical infrastructure and cybersecurity, in particular the adoption of the CER and NIS2 Directives. While it is not surprising that the Strategy calls for the urgent transposition of these Directives, it further envisages that the Commission will engage with Member States to identify additional sectors and services not covered by the current legislation where there may be a need to act, e.g., Europe's defence industrial base.[47]

A notable action put forward by the Strategy, also referred to in Niinistö's report, concerns the embedding of a *Preparedness and Security by Design* principle in future EU legislation, policies, and programmes. This approach slightly deviates from the recommendation put forward in the report, which called for an explicit security and preparedness check in all future impact assessments accompanying new legislative initiatives proposed by the Commission. Taken together with the principles of proportionality in combination with the Commission's objective in the Competitiveness Compass to simplify EU rules, the Strategy takes a more targeted approach, namely that future initiatives should be developed with preparedness and security perspective considerations in mind. The true value and implications of this approach will be revealed through practical application on a case-by-case basis in specific initiatives.

Peace through defence?

A number of recommendations put forward by the Niinistö and Draghi reports particularly focused on defence. The response to these recommendations is evident in the **joint White Paper for European Defence Readiness 2030**[48] of the European Commission and the High Representative published on 19 March 2025. Against the background of the immense disruption of the post-Cold War political order currently taking place and the systematic under-investment in Europe's defence capabilities, the White Paper sets out a framework to strengthen European defence and to support Ukraine. The actual novelty of the White Paper is the launch of the ReArm Europe Plan, an urgent defence response plan with six measures to speed up defence spending in the EU: a new EU regulation to provide Member States with loans backed by the Union budget; a proposal to activate the National Escape Clause allowing Member States to mobilise additional defence expenditure, which could reach at least €800 billion over the next four years; additional incentives granting more flexibility and incentives to increase European defence investments; further contributions by the European Investment Bank, including a widening of the scope of defence-related funding; the mobilisation of private capital, including through the Savings and Investment Union; and the exploration of additional funding sources for defence, notably under the next Multiannual Financial Framework.[49]

With the objective of ensuring European defence readiness by 2030 at the latest, the White Paper provides concrete directions for invigorating the Union's defence technological and industrial base, stimulating research, and creating an EU-wide market for defence equipment. While Member States' defence spending has significantly increased over the years and is currently estimated at 1.9% of the EU's combined GDP (€326 billion in 2024),[50] it is still considered insufficient in the new era of security threats fuelled by geographical, geopolitical, technological, and competitive motives.

ProtectEU: safeguarding the EU's internal security

The latest building block in the new security architecture designed by the Commission concerns the European Internal Security Strategy adopted on 1 April 2025.[51] Branded as **"ProtectEU"**, this new strategy continues the foundational work laid out in the Security Union Strategy, despite use of the term "internal", and does not exclusively focus on the classical internal security threats (updating the Framework Decision on organised crime, strengthening Europol, and the adoption of new, targeted strategies and action plans in the areas of counterterrorism, and trafficking in firearms, drugs, and humans as well as the protection of children against crime). ProtectEU not only addresses threats posed by organised crime and terrorism but also puts the spotlight on hybrid threats, including incidents affecting the EU's critical infrastructure, cyber-attacks, disinformation, and foreign interference.

The Strategy of 1 April 2025 establishes a **new governance model** for European internal security.[52] This is done through consolidation of the principle that security should be mainstreamed in all the EU's future actions, in line with the Preparedness Union Strategy adopted at almost the same time. Regular meetings of the Commission Project Group on European Internal Security, enhanced by strategic cross-sectoral collaboration at the service level, should enable the Commission to embed the notion of security in all aspects of its work. The new format of the Commission's Security College will duly discuss internal security elements and their potential impact on different policy areas. To ensure the necessary transparency on progress made in implementing the actions put forward, the Strategy requires that the Commission regularly update the Council and European Parliament. Regular EU internal security threat assessments based on sectoral analysis should feed into the EU's comprehensive risk and threat assessment, as announced in the Preparedness Union Strategy.

The ProtectEU Strategy acknowledges that the online and offline dimensions of security have currently become blurred and puts a strong emphasis on digital risks and vulnerabilities, such as cybersecurity and cybercrime. In this context, the Commission also proposed an updated Cybersecurity Blueprint[53] on cybersecurity crisis management that, once adopted by the Council, would provide a solid framework for cyber crisis management. While it does not introduce new mechanisms and tools as such, it does present in a clear and simple manner how to make use of available mechanisms across the full crisis management lifecycle. The Action Plan on the Cybersecurity of Hospitals and Healthcare Providers[54] is another example of the need to accelerate collective action in particularly vulnerable areas. Moreover, the Strategy announces actions in the field of access to data by law enforcement, including the preparation of an impact assessment with a view to updating rules on data retention at Union level.

The Strategy reinforces that attempts to decouple internal and external security aspects are not feasible in the current context: threats originating outside the EU have a direct impact on the lives of European citizens. For example, drugs produced in Latin America and illegally trafficked to Europe end up in European cities and towns, thus inevitably increasing insecurity close to home. Geopolitical events, such as the new Taliban regime in Afghanistan and the fall of the al-Assad regime in Syria generate changes in drug trafficking routes

https://doi.org/10.30709/eucrim-2025-004

and increase terrorist threat levels across Member States. Incidents in undersea critical infrastructure in the Baltic States have the potential to disrupt a larger range of critical and essential services in Europe, such as energy supply and telecommunication services. In response to these latter incidents, the Commission and the High Representative presented an Action Plan to enhance the security and resilience of submarine cables.[55]

IV. Views from other EU Institutions and Actors in the Area of Security

Shaping the EU's security is not a task which can be carried out by the Commission alone. Co-legislators, Member States' authorities and other actors including EU agencies and bodies operating in this area carry an important responsibility in materialising the EU's security architecture. This section provides an overview of their main positions.

The **Council** adopted in December 2024 **strategic guidelines** for the next five years in the area of freedom, security and justice[56]. The fact that these guidelines focus on implementation should not be seen as a lack of ambition, given the complexity and number of legislative and policy instruments adopted in recent years. The 39 guidelines provide useful insight into the Council's position in both a general and specific sense. For example, with regard to serious and organised crime, specifically the fight against corruption, the guidelines underline the continued need to focus on and implement the recommendations put forward by the High-level Group on access to data for effective law enforcement (e.g., the adoption of rules on data retention). In light of the EU's challenges related to the changing security landscape worsened by global conflicts and climate change, the guidelines also point out that initiatives in the Justice and Home Affairs area should contribute to strengthening preparedness and crisis response at Union level. With "Security, Europe" as its core motto, the Polish Presidency of the Council of the European Union had set this specific area at the heart of the EU's priorities.

In recent years, **the European Parliament** has adopted a number of resolutions reflecting its position on EU security. As co-legislator, it recently adopted a resolution on the White paper on the future of European defence.[57] Specifically, this resolution calls on the EU to invest substantially more in defence, to integrate a defence and security dimension in *most* Union policies,[58] and to embed a *Preparedness by Design* principle horizontally and consistently across EU institutions, bodies, and agencies. Earlier resolutions – following Commission strategies and actions in the area of organised crime,[59] cybersecurity,[60] and the Security Union Strategy[61] – offer further guidance on the Parliament's priorities. Having reflected on the new opportunities for fraud with EU funds following the COVID-19 pandemic (in connection to the disbursement of NextGenerationEU), the European Parliament also emphasised the need to step up the fight against organised crime at the Union and national levels and called on the Commission to revise the Framework Decision on the fight against organised crime.[62] As regards the issue of funding, a visible difference exists between the Parliament's approach towards cybersecurity versus the traditional justice and home affairs policies. While for cybersecurity and related infrastructure deployment, the Parliament calls for a coherent use of EU funds and the need to exploit synergies between different EU programmes;[63] it expresses deep concerns and calls for adequate funding and staffing of EU Justice and Home Affairs agencies and bodies in order for the EU to deliver on the Security Union Strategy.[64]

EU agencies and bodies operating in the security sphere carry an important responsibility in forming future policy to prevent, anticipate, and respond to cross-border threats. Europol's most recent Serious and Organised Crime Threat Assessment report 2025[65] identifies cyber-attacks, online fraud schemes, (online) child sexual exploitation, migrant smuggling, drug trafficking, firearms trafficking, and waste crime as key

https://doi.org/10.30709/eucrim-2025-004

threats. According to Europol, a particularly worrying and recent trend concerns the increased collaboration between criminal networks and hybrid threat actors. Guidance on the terrorism situation and trends in Europe is provided by, for example, the European Union Terrorism Situation and Trend Report.[66] Such terrorism and situation trend reports provide input for the future EU Counter-terrorism Agenda, which will need to reflect on the rise in terrorist attacks, the increased use of technological innovations such as Artificial Intelligence, and the active involvement of young individuals in terrorism and violent extremism. The increase in cyber-attacks and crimes committed through online means, notably ransomware and malware attacks, is also highlighted in the most recent ENISA Threat Landscape report.[67] All these agencies make an important contribution to shaping the EU's priorities in the area of security by raising situational awareness in their operational activities.

V. Conclusion

The increased attention to security across the EU, particularly in the current threat landscape, should be welcomed. However, the consolidation of the EU's cross-cutting approach to security has translated into a growing number of initiatives dealing with this topic, leaving the notion as open as it is salient.

In contrast with the previous Commission mandate, when the Security Union Strategy served as a comprehensive umbrella for the EU's security policy, there is currently no single initiative to bring together all security matters. In addition to the recently adopted Preparedness Union Strategy and Internal Security Strategy, there are also sectoral strategies, such as those related to economic security, maritime security, and energy security. While the proposed initiatives raise security concerns to the highest political level, it remains to be seen how this will be organised in a clear and convincing way, ensuring streamlining and coordination.

An efficient legislative and operational environment, with enhanced clarity on the role, responsibilities, added value, and complementarities of the various actors in the security landscape, is indispensable and urgent. The operationalisation of the mainstreaming of security and preparedness into future EU policies and initiatives, as announced in the Preparedness Union Strategy and the Internal Security Strategy, may reveal how the EU's concept of security will be further framed. Such clarity is a prerequisite for the trust necessary when providing an integrated and holistic approach to existing and potential security challenges.

With the concept of security inherent to a wide range of different instruments, actions, and policy areas, there is a constant risk of overlaps, divergencies in interpretation, and a duplication of efforts that must be avoided if the EU is to live up to its responsibility under the Treaties to protect citizens. While certain areas (such as the protection of critical infrastructure) are recognised in multiple strategies, other areas (such as the dependencies on high-risk vendors for the provision of critical services, materials, technology, and equipment) have not received the same concerted attention. Such gaps need to be addressed in a systematic way.

Stronger governance would also help address the challenge of funding for security policies and agencies, particularly in view of the upcoming negotiations on the next multiannual financial framework. A clear prioritisation and political will is needed to balance specific priorities, such as the strengthening of Europol and Frontex with new initiatives, e.g., the ReArm Europe plan to mobilise up to €800 billion for defence investment and the InvestAI initiative to mobilise €200 billion of investment in Artificial Intelligence.

Another point for consideration concerns the need to balance the work on preparing and negotiating new initiatives versus the need to timely and correctly implement agreed legislation. Without proper implementation and enforcement, legislative instruments and policies risk losing their impact in practice. Urgent political developments necessitate prompt adaptation and reaction at the EU and national levels. The EU level added value, and the merit of effective governance on these issues, thereby resides in ensuring stronger coordination, resource and intelligence pooling, increased collective efficiency, and a scale effect, building on Member States' efforts.

Ultimately, while security may not be better assured through the development of a firm construct or concept, vigilance remains of the essence for the EU in order to maintain a horizontal overview and ensure a coordinated approach towards the protection of its own security, especially in today's times.

---

1. Cf. Art. 2 TEU: "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail." Art. 3(1) TEU: "The Union's aim is to promote peace, its values and the well-being of its peoples."↩
2. Art. 67(3) TFEU: "The Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws."↩
3. Art. 4(2) TEU: "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."↩
4. Communication from the Commission to the European Parliament and the Council, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* COM(2010) 673 final.↩
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security*, COM(2015) 185 final.↩
6. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Security Union Strategy*, COM(2020) 605 final.↩
7. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.↩
8. On 3 May 2023, the Commission adopted a package with legislative and policy measures to strengthen the fight against corruption (see also the news in *eucrim* 2/2023, 139-141). While the directive on combatting corruption is currently under trilogue negotiations by co-legislators, multiple actions proposed by the Joint Communication on the fight against corruption (JOIN(2023) 12 final) have been adopted, including the setting up of an EU Network against Corruption.↩
9. Proposal for a Regulation of the European Parliament and of the Council on enhancing police cooperation in relation to the prevention, detection and investigation of migrant smuggling and trafficking in human beings, and on enhancing Europol's support to preventing and combating such crimes and amending Regulation (EU) 2016/794, COM(2023) 754 final; Proposal for a Directive of the European Parliament and of the Council laying down minimum rules to prevent and counter the facilitation of unauthorised entry, transit and stay in the Union, and replacing Council Directive 2002/90/EC and Council Framework Decision 2002/946 JHA, COM(2023) 755 final.↩
10. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, COM(2020) 795 final.↩
11. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Strategy to tackle Organised Crime 2021-2025*, COM(2021) 170 final.↩
12. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *EU Agenda and Action Plan on Drugs 2021-2025*, COM(2020) 606 final.↩
13. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025*, COM(2021) 171 final.↩
14. Communication from the Commission to the European Parliament and the Council *on the Seventh Progress Report on the implementation of the EU Security Union Strategy and Annex*, COM(2024) 198 final.↩
15. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, OJ L 333, 27.12.2022, 164.↩
16. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, 80.↩
17. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.↩
18. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025.↩
19. For more information on the E-evidence package: A. Juszczak and E. Sason, "The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice – An Introduction to the New EU Package on E-evidence", (2023) *eucrim*, 182-200.↩

[20] Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, OJ L, 2024/1712, 24.6.2024.↩

[21] Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC, OJ L, 2024/1203, 30.4.2024. For details and comments on this Directive, see the articles in the special *eucrim* issue no. 2/2024 ("Protection of the Environment").↩

[22] New rules to tackle anti-money laundering and terrorism financing (AML/CFT) together with the Regulation establishing the new Anti-Money Laundering Authority (AMLA) were published in the Official Journal on 19 June 2024. See also the news in *eucrim* 2/2024, 113-120.↩

[23] Directive (EU) 2024/1260 of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation, OJ L, 2024/1260, 2.5.2024.↩

[24] Europol, *European Union Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime*, 2025, p. 26.↩

[25] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation), OJ L, 2024/982, 5.4.2024.↩

[26] Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA, OJ L 134, 22.5.2023, 1.↩

[27] Council Recommendation (EU) 2022/915 of 9 June 2022 on operational law enforcement cooperation, OJ L 158, 13.6.2022, 53.↩

[28] Council of the European Union, *A Strategic Compass for Security and Defence – for a European Union that protects its citizens, values and interests and contributes to international peace and security*, Council document 7371/22 of 21 March 2022. Available at: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf> accessed 10 June 2025.↩

[29] Ibid, pp. 13, 23-24, 28, 32, 37, 44.↩

[30] All seven progress reports on the implementation of the Security Union Strategy 2020-2025 are available here: <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en> accessed 10 June 2025.↩

[31] Communication from the Commission to the European Parliament and the Council *on the Seventh Progress Report on the implementation of the EU Security Union Strategy*, COM(2024) 198 final.↩

[32] Ibid, pp. 22-23.↩

[33] Ibid, p. 24.↩

[34] Ibid, p. 22.↩

[35] Europe's choice. Political Guidelines for the next European Commission 2024-2029. Ursula von der Leyen, Candidate for the European Commission President. Published on 18 July 2024, available at: < https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf> accessed 10 June 2025.↩

[36] During the past few years, there have been several suggestions from different stakeholders on areas to which the EPPO's competences could be extended. On 12 September 2018, the Commission adopted a Communication, including an initiative to extend the competences of the EPPO to cross-border terrorist crimes. See, for more information on this initiative: A. Juszczak and E. Sason, "Fighting Terrorism through the European Public Prosecutor's Office (EPPO)? What future for the EPPO in the EU's Criminal Policy?", (2019) *eucrim*, 66-74.↩

[37] Press remarks by President von der Leyen on the first 100 days of the 2024-2029 Commission, 9 March 2025, <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_25_721> accessed 10 June 2025.↩

[38] An overview of the mission letters to Commissioners-designate can be found at: Commissioners-designate (2024-2029) – European Commission, <https://commission.europa.eu/about/commission-2024-2029/commissioners-designate-2024-2029_en> accessed 10 June 2025.↩

[39] The Draghi Report: The future of European competitiveness, September 2024, available at: <https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en> accessed 10 June 2025.↩

[40] Ibid, p. 17.↩

[41] Enrico Letta, *Much more than a market. Speed, security and solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, April 2024, available at: <https://single-market-economy.ec.europa.eu/news/enrico-lettas-report-future-single-market-2024-04-10_en> accessed 10 June 2025.↩

[42] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Competitiveness Compass for the EU*, COM(2025) 30 final.↩

[43] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness. Report by Sauli Niinistö, former President of the Republic of Finland, in his capacity as Special Adviser to the President of the European Commission, available at: <https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en> accessed 10 June 2025.↩

[44] Ibid, p. 7.↩

[45] European Commission & High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions *on the European Preparedness Union Strategy*, JOIN(2025) 130 final.↩

[46] (1) Foresight and anticipation; (2) resilience of vital societal functions; (3) population preparedness; (4) public-private cooperation; (5) civil-military cooperation; (6) crisis response coordination; and (7) resilience through external partnerships.↩

[47] Niinistö Report, *op. cit.* (n. 43), p. 21.↩

[48] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Joint White Paper for European Defence Readiness 2030*, JOIN(2025) 120 final.↩

[49] Ibid, pp. 17-19.↩

[50] Ibid, p. 16.↩

[51] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *on ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final.↩

[52] Ibid, p. 3.↩

[53] Proposal for a Council Recommendation for an EU Blueprint on cybersecurity crisis management, COM(2025) 66 final.↩

[54] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *European action plan on the cybersecurity of hospitals and healthcare providers*, COM(2025) 10 final.↩

[55] Joint Communication of the European Commission and High Representative of the Union for Foreign Affairs and Security Policy: *EU Action Plan on Cable Security*, JOIN(2025) 9 final.↩

[56] Strategic guidelines for legislative and operational planning within the area of freedom, security and justice adopted at the Justice and Home Affairs Council on 12 December 2024, Council document 16343/24.↩

[57] European Parliament resolution of 12 March 2025 on the White Paper on the Future of European Defence (2025/2565(RSP)), P10_TA(2025)0034.↩

[58] Ibid, point 9.↩

[59] European Parliament resolution of 15 December 2021 on the impact of organised crime on own resources of the EU and on the misuse of EU funds with a particular focus on shared management from an auditing and control perspective (2020/2221(INI)), P9_TA(2021)0501.↩

[60] European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)), P9_TA(2021)0286.↩

[61] European Parliament resolution of 17 December 2020 on the EU Security Union Strategy (2020/2791(RSP), P9_TA(2020)0378.↩

[62] Ibid, point 8: "reiterates its previous calls for the revision of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime, and the need to establish a common definition of organised crime; considers that this common definition should also take into account the use of violence, corruption or intimidation by criminal groups to obtain control of economic activities or public procurement, or to influence democratic processes."↩

[63] European Parliament resolution of 10 June 2021, op. cit. (n. 60), point 7.↩

[64] European Parliament resolution of 17 December 2020, op. cit. (n. 61), point 42: "Is deeply concerned by the lack of resources allocated to some EU agencies acting in the field of justice and home affairs (JHA) to comply fully with their mandate; calls for proper funding and staffing of EU agencies and bodies in the field of JHA in order for the EU to deliver on the Security Union Strategy."↩

[65] Europol SOCTA, 2025, *op. cit.* (n. 24).↩

[66] Europol (2024), European Union Terrorism Situation and Trend Report, Publications Office of the European Union, Luxembourg.↩

[67] The ENISA Threat Landscape 2024 covered the period from July 2023 to June 2024 and was published in September 2024. The primary cybersecurity threats identified are: ransomware, malware, social engineering, threats against data, threats against availability: Denial of Service, information manipulation and interference, and supply chain attacks.↩

Authors statement

The views expressed in this article are solely those of the authors and are not an expression of the views of their employer or the institution they are affiliated with.

Views and opinions expressed in the material contained in eucrim are those of the author(s) only and do not necessarily reflect those of the editors, the editorial board, the publisher, the European Union, the European Commission, or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the European Commission are not responsible for any use that may be made of the information contained therein.

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

https://doi.org/10.30709/eucrim-2025-004

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union

https://doi.org/10.30709/eucrim-2025-004