Council of the
European Union

Brussels, 27 May 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	25 May 2022
To:	General Secretariat of the Council
No. Cion doc.:	COM(2022) 252 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Fourth Progress Report on the implementation of the EU Security Union Strategy

Delegations will find attached document COM(2022) 252 final.

Encl.: COM(2022) 252 final

EUROPEAN
COMMISSION

Brussels, 25.5.2022
COM(2022) 252 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Fourth Progress Report on the implementation of the EU Security Union Strategy

I. INTRODUCTION

The Russian war of aggression against Ukraine dominates today's EU security agenda. The war not only threatens Ukraine, but seeks to damage global stability and security. Inside the EU, it brings a range of risks to the security of citizens. There are new uncertainties over supplies of energy and other raw materials, and critical infrastructure may be targeted in cyberattacks. EU internal safety and security are jeopardised by potential attacks or accidents resulting from chemical, biological, radiological or chemical agents in the war zone. The vulnerabilities of millions of people who have fled the war can be quickly exploited by organised crime, through trafficking of women and children, who are particularly at risk.

In the face of these new and potential threats, the EU has remained resolute and united. While the impact of the war has so far remained principally limited to the territory of Ukraine, the EU has stepped up *vigilance and coordination* with increased monitoring of the threat landscape, and has worked to strengthen resilience to ensure *preparedness*.

In the Versailles Declaration of 10-11 March 2022[1], European leaders stressed the need to prepare for fast-emerging challenges, including by "protecting ourselves against ever-growing hybrid warfare, strengthening our cyber-resilience, protecting our infrastructure – particularly our critical infrastructure – and fighting disinformation".

The Security Union framework is central to ensuring security across the EU. The four strategic priorities set out in the Security Union Strategy[2] remain directly relevant to this task in the current geopolitical context: (i) a future proof security environment; (ii) tackling evolving threats; (iii) protecting Europeans from terrorism and organised crime; and (iv) a strong European security ecosystem. The war has underlined the need for the EU and its Member States to make full use of legislative and policy instruments already available under the Security Union Strategy, which underpin coordinated EU support to Member States on issues from organised crime and terrorism, to cybersecurity and hybrid threats.

The European agencies in the area of Justice and Home Affairs have also stepped up their efforts in response to the war in Ukraine, playing a key role in assessing threats and in supporting operational responses[3]. Continuous strengthening of the Schengen area's operational practice and governance is another important factor.

This fourth Security Union progress report focuses on the developments over the past few months since the Russian war of aggression against of Ukraine. It provides an overview of actions taken on all Security Union strands and considers the preparedness needs arising from potential security threats stemming from the war in Ukraine. Progress on other Security Union files can be found in annex.

---

1 https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf

2 COM/2020/605.

3 Joint Statement from EU Justice and Home Affairs Agencies on Ukraine | European Union Agency for Asylum (europa.eu)

II. CYBERSECURITY AND CRITICAL INFRASTRUCTURE

Since the outbreak of the war, private actors and criminal operations have publicised the fact that they are undertaking cyber activities in support of one side or the other. Hacktivism[4] poses a threat due to the risk of spill-over effects in the EU against critical services, the risk of attacks coming from official networks or other unforeseen spill-over effects. While so far, the war has largely been waged through conventional means with only limited spill-over effects, the risk of escalation in this area is real.

The EU has therefore stepped up its coordination and preparedness. The threats arising from the war underline the need to build a culture of sharing information and expertise between the EU, the Member States, and across the cybersecurity communities. This includes building an integrated situational awareness, shared by the EU institutions, bodies and agencies and Member States, in particular for the critical infrastructure on which the smooth functioning of the internal market depends.

Attribution of cyber-attacks against Ukraine

Cyber-attacks on Ukraine itself began before the Russian aggression, and in the first days of the war,[5] aimed to compromise user accounts of Ukraine's military personnel and disrupt the essential services including border control and telecommunications.

On 14 January 2022, the High Representative made a Declaration[6] on behalf of the European Union condemning the cyberattacks against Ukraine and reconfirming the EU's unequivocal support to Ukraine.

On 10 May, the European Union and its Member States, together with international partners strongly condemned[7] the malicious cyber activity against Ukraine on 24 February, which targeted the satellite KA-SAT network, owned by Viasat, and directly attributed the attack to the Russian Federation. This cyberattack had a significant impact, causing indiscriminate communication outages and disruptions across several public authorities, businesses and users in Ukraine, as well as affecting several EU Member States.

Vigilance and coordination

Since Russia's war of aggression against Ukraine, the monitoring of the cybersecurity situation in Member States and EU institutions has increased. ENISA, the EU Agency for Cybersecurity, the European Cybercrime Centre of Europol and CERT-EU, the Computer Emergency Response Team for EU Institutions, Bodies and Agencies and the EU Intelligence

[4] A recent example of hacktivism is the use of "protestware" to spread malware to Russian IPs through a popular open source package, which could lead to supply chain risks and loss of trust in the open source community. The Commission has made clear that (even well-intentioned) cyberattacks on Russia are illegal.

[5] Microsoft Special Report: An overview of Russia's cyberattack activity in Ukraine; The hybrid war in Ukraine - Microsoft On the Issues

[6] https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/

[7] Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - Consilium (europa.eu)

and Situation Centre (EU INTCEN), have all contributed to the EU's shared situational awareness, including by providing regular monitoring of suspicious cyber activity, including in specific sectors such as energy, transport and aviation, and have provided assessments to guide preventive action.

There has also been intensified coordination and exchange of information with cybersecurity networks, such as the Cyber Crises Liaison Organisation Network (CyCLONe) comprising national cybersecurity agencies, the Commission and ENISA. To reflect this approach internally in the EU institutions, a coordinating mechanism, the Cyber Crisis Task Force, enables information to be shared among all relevant services and bodies and agencies, including ENISA, EUROPOL's European Cybercrime Centre and CERT EU. Constant efforts are needed to ensure channels of communication between the political, operational and technical levels, as well as to enhance cooperation with the Computer Security Incident Response Teams (CSIRT) Network.

Europol also triggered the EU Law Enforcement Emergency Response Protocol that enables reinforced cyber threat monitoring and information-sharing amongst a broad range of stakeholders to build a comprehensive cyber intelligence picture.

Beyond cyber threats, there is intensified vigilance by Member States, EEAS and the Commission services concerning the exposure of critical infrastructures to non-cyber, physical threats. Critical infrastructures and entities that operate them may be exposed to physical risks, such as sabotage by the state or by state-sponsored actors as part of possible retaliatory measures against the EU.

Preparedness

Preparedness in the area of cybersecurity and security of critical infrastructure is more essential than ever, given the increased exposure of Europe to an accumulation of threats due to the war. Efforts to step up preparedness has included a number of direct actions, including some that were already foreseen before Russia's aggression against Ukraine. These include exercises, guidance, legislative measures, increasing resilience in critical sectors, and work with partners.

The French Presidency of the Council of the European Union, together with the European External Action Service (EEAS) and the European Union Agency for Cybersecurity (ENISA) organised a scenario-based exercise in early 2022, called EU CyCLES (Cyber Crisis Linking Exercise on Solidarity), with the aim of raising awareness at the political level and strengthening cooperation between the operational and political levels in case of a large-scale cyber-attack.

ENISA and CERT-EU published **guidelines** in February, on how to increase resilience and preparedness in the EU[8]. These encourage all public and private sector organisations in the EU to adopt a minimum set of cybersecurity best practices to substantially improve cybersecurity culture. In March, CERT-EU published follow-up technical guidance, with ENISA's support[9], as well as a security guidance for strengthening the configuration of

[8] Boosting your Organisation's Cyber Resilience - Joint Publication, 14.02.2022.
[9] Security Guidance 2022-01 - Cybersecurity mitigation measures against critical threats.

Signal apps[10] with a number of practical recommendations to organisations to improve their cybersecurity posture.

Legislative initiatives

The current situation underlines the urgency to **implement existing legislation**, and to accelerate the **adoption of pending initiatives**.

The Commission is supporting Member States in implementing the **NIS Directive**[11], which requires Member States to be appropriately equipped, for example with a Computer Security Incident Response Team (CSIRT) and by defining competent authorities. It provides a basis for effective cooperation between Member States. The political agreement found by the co-legislators on the **NIS2 Directive**[12] is a further breakthrough in providing a robust EU framework of preparedness.

NIS 2 - further strengthening preparedness

- The new Directive on Network and Information Systems will address deficiencies of the previous NIS Directive, to adapt it to the current needs and make it future-proof. It sets out minimum rules for a regulatory framework and lays down mechanisms for effective cooperation among relevant authorities in each Member State.
- It widens the scope of the rules, with new sectors critical for the economy and society added (for instance, the pharmaceutical and medical devices sectors or food manufacturing). All medium-sized and large entities operating within the sectors or providing services covered by the directive will fall within its scope. Public administration entities of central governments (excluding the judiciary, parliaments and central banks) and at regional level are also covered. In addition, Member States may decide that it applies to such entities at local level.
- NIS2 will set the baseline for cybersecurity risk management measures and formally establishes the European Cyber Crises Liaison Organisation Network, EU-CyCLONe, which will support the coordinated management of large-scale cybersecurity incidents.
- The proposal also introduces more precise provisions on the process for incident reporting, the content of the reports and timelines, and provides for remedies and sanctions to ensure enforcement.
- Member States will have 21 months from the entry into force of the directive in which to incorporate the provisions into their national law.

Progress on NIS 2 should be followed as soon as possible by completion of negotiations on the proposed **Directive on the resilience of critical entities**[13] ('CER Directive'), which, once adopted and implemented, should increase the resilience of critical entities to a range of threats, including terrorist attacks, insider threats or sabotage. It is also essential that the level of ambition of the Directive on the resilience of critical entities matches that of the Commission proposal, and that consistency is maintained with the political compromise found on NIS2. Together these measures will boost resilience and preparedness by putting in place a more coherent and robust system including through national incident and crisis

[10] CERT-EU Security Guidance 22-002 - Hardening Signal.
[11] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[12] COM(2020) 823.
[13] COM(2020) 829.

response plans. These were also part of the Commission Recommendation of last year[14] creating the **Joint Cyber Unit**, which set out how the different actors of the cybersecurity ecosystem (diplomatic, police, civilian and, where appropriate, defence) are to cooperate on an operational level. The current threat landscape underlines the value of such effective cooperation between key players.

The Commission continues to monitor the implementation of the toolbox on cybersecurity of **5G**[15]. In this context, on 11 May the NIS Cooperation Group adopted a report on the security of OpenRAN[16]. It also continues working together with Member States, to make the European cybersecurity competence centre fully operational.

On 22 March 2022, the Commission proposed **new rules to establish common cybersecurity and information security measures across the EU Institutions, Bodies and Agencies (EUIBA)**. These rules will bolster the EU administration's resilience and ability to respond to cyber threats and incidents. By placing these activities in a common framework, inter-institutional cooperation will be strengthened, and risk exposure minimised. The proposed **Cybersecurity Regulation for EUIBAs**[17] will enhance the mandate of CERT-EU and lead to the creation of a new inter-institutional Cybersecurity Board, boost cybersecurity capabilities, and stimulate regular maturity assessments and better cyber-hygiene. The proposed **Information Security Regulation**[18] will create a minimum set of information security rules and standards for the secure handling and exchange of information of all EUIBAs to ensure an enhanced and consistent protection against the evolving threats to their information. The Commission calls on the European Parliament and the Council to swiftly adopt these measures.

The Commission has now completed its public consultation on measures to boost the **Cyber resilience** of digital products, preparing a proposal to be published this autumn[19]. This will address the vulnerabilities of digital products and ancillary services that – while they create opportunities for EU economies and societies – also lead to new challenges since the more everything is connected, the easier it is for a cybersecurity incident to affect an entire system, and thus to disrupt economic and social activities.

On 9 March 2022, the EU ministers in charge of telecommunications unanimously adopted the Nevers Call to Reinforce the EU's Cybersecurity Capabilities, which included "the implementation of a new Emergency Response Fund for Cybersecurity to be put in place by the Commission"[20]. The Commission is reflecting on the best use of existing funds to support preventive and response actions.

Critical sectors

---

14 Recommendation on building a Joint Cyber Unit | Shaping Europe's digital future (europa.eu)
15 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
16 NIS Cooperation Group, Report on the cybersecurity of Open RAN, 11 May 2022.
17 COM(2022) 122.
18 COM(2022) 119.
19 Cyber resilience act – new cybersecurity rules for digital products and ancillary services (europa.eu)
20 08/03/2022 - Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances (economie.gouv.fr)

The security of the EU's **energy** supply is critical to citizens' well-being, and to the smooth functioning of our economies, and the current situation has highlighted the need for clear rules on cyber security in in this sector. The Commission is working on a Network Code on cyber-security for cross-border electricity flows as required by the Electricity Regulation[21], to provide rules on risk assessments, common minimum requirements, planning, monitoring, reporting and crisis management. Since Russia's war of aggression against Ukraine, the objectives intended for the network code on cybersecurity are even more relevant. The Commission has also launched a structural cooperation between ENISA, ENTSO-E[22], ENTSOG[23] and the Energy Community in the regular monitoring of the cybersecurity situation in the energy sector.

The EU has worked to protect partners' security without creating new risks for itself. The emergency synchronization of the electricity grids of Ukraine and Moldova with the Continental Europe Grid took place in March 2022 after the adoption of risk mitigating measures, notably in terms of cybersecurity.

The war and sanctions have also created many challenges for EU **transport**, from safety risks for EU civil aviation and truck drivers stuck in conflict zones, to the destruction of Ukrainian transport infrastructure, cutting off supply chains and threatening global food security. The European Union Aviation Safety Agency, in close cooperation with the Commission and Eurocontrol, the European Organisation for the Safety of Air Navigation, have advised operators since the start of the war not to operate within the airspace of Ukraine and avoid using the airspace within 100 nautical miles of the Belorussian and Russia/Ukraine border.

The Commission has also been working to strengthen the preparedness and resilience of the EU transport sector. In particular a new Contingency plan for transport[24], adopted on 23 May, draws lessons from both the COVID-19 pandemic and Russia's military aggression against Ukraine. It proposes a toolbox of 10 actions to guide the EU and its Member States when introducing emergency crisis-response measures, including ensuring minimum connectivity, building cyber and hybrid threats resilience and enhancing cooperation with international partners on crisis preparedness and response. It also highlights the importance of regular resilience testing for different crisis scenarios, bringing together relevant EU agencies or other actors, and building on existing processes.

Under the **EU Health security** framework, the exchange of information based on the Early Warning and Response System, including support for medical evacuations from Ukraine, must be protected against cyberattacks, hence the system's security is being reinforced.

Cooperation with partners

The EU continues to work with its international partners to prevent, discourage, deter and respond to malicious behaviour in cyberspace. Russia's war of aggression against Ukraine has made cooperation in this field more important than ever. In this regard, the EEAS has been working to exchange situational awareness and coordinate response to malicious cyber activities targeting Ukraine, as well as on support to Ukraine and others in the region, by

[21] Regulation (EU) 2019/943 of the European Parliament and the Council of 5 June 2019 on the internal market for electricity, OJ L158, 14.6.2019, p.54. A proposal is currently under review by the Agency for the Cooperation of Energy Regulators.

[22] European Network of Transmission System Operators for Electricity.

[23] European Network of Transmission System Operators for Gas.

[24] COM(2022) 21.

working with partners including US and NATO to ensure complementarity and avoid overlaps.

Close cooperation with the US also intensified in the context of the EU-US Trade and Technology Council (TTC). The Joint Statement[25] following the Ministerial meeting in Paris in May, emphasised the central role of the TTC for the renewed transatlantic partnership, which serves to coordinate joint measures by the EU and the US in face of the Russian aggression against Ukraine. Both parties agreed that close cooperation to advance the resilience of supply chains is more important than ever. In addition, a dedicated taskforce on public financing for secure and resilient digital infrastructure in third countries was established to pave the way to joint US-EU public financing of digital projects in third-countries, based on a set of common overarching principles.

The Strategic Compass adopted in March 2022 (see section VII) will further strengthen the EU Cyber Diplomacy Toolbox and develop the EU Cyber Defence Policy to be better prepared for and respond to cyberattacks, as part of a broader strategy to strengthen EU ability to act in crises and defend its interests.

Cybersecurity support to Ukraine and neighbouring countries

The EU was already supporting Ukraine's cyber resilience before the war. Already in June 2021, the EU and Ukraine held a first Cyber Dialogue, and. the EU provided support to cyber security and resilient digital transformation via the EU4Digital Ukraine programme worth €25 million. A further €1.5 million twinning programme is designed to help Ukraine's cybersecurity institutions align with EU standards.

Following the outbreak of war, the EU is promoting co-operation between EU and Ukrainian cyber experts, and coordinating provision of technical assistance, equipment, software and relevant services, to strengthen Ukraine's cyber resilience and cyber defence.

In addition, the EU is working to assess possible support medium-term support to Moldova, Georgia and Western Balkans. A joint assessment mission to Moldova on cybersecurity needs was conducted on 3-4 March 2022 and has led to the adoption of a dedicated crisis response measure to rapidly scale up cyber security in the country. Similar rapid response support is being prepared for a select number of countries in the Western Balkans, considered to be particularly risk-exposed as a result of their alignment with EU-sanctions. Possible additional assistance to Moldova through the European Peace Facility is also being assessed.

III. ORGANISED CRIME AND TERRORISM

Russia's war of aggression against Ukraine has forced millions of people to leave their homes, vastly increasing movements across the EU's external borders. By 18 May, nearly 6 million had arrived to the EU from Ukraine and Moldova, and to date 2.8 million have registered for temporary protection in the EU. The EU has sought to provide the swiftest and most flexible reception to those fleeing the war, without compromising security at the EU's external border. The EU has taken unprecedented measures to offer those fleeing the war

[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108

temporary protection, and is committed to handling all new arrivals without discrimination. At the same time, the potential risks that may arise from so many people on the move cannot be neglected, and the EU, with strong support from the relevant EU agencies, remains vigilant as to new developments in organised crime and terrorism.

A strong Schengen at a moment of increased threats

Ensuring a high level of security in the **Schengen** area and within the EU, has never been as important as in the atmosphere of heightened threats arising from the war just beyond the EU's external border.

Delivering on the ambitious agenda for the Schengen area set out in the strategy of June 2021, the Commission adopted in May the first State of Schengen report[26]. The annual Schengen Cycle provides a new governance model for the Schengen area, with a regular health check on the state of Schengen. This will help ensure prompt identification of shortcomings and efficient follow-up procedures, in order to make the Schengen area stronger and more resilient.

This first report acknowledges the need to strengthen efforts to implement key EU-level initiatives including systematic checks at the external borders of all travellers, making full use of the Frontex and Europol mandates, as well as proposed and available cross-border police cooperation tools.

In particular, the new architecture for EU information systems for borders, migration and security, and their interoperability, is the cornerstone of efforts to improve internal security and border management. Effective implementation of all elements of the interoperability framework in line with agreed timelines will be crucial.

Vigilance and coordination

Stronger law enforcement cooperation across Member States and with third countries is key to ensure awareness of emerging criminal and terrorist threats, and action on criminal networks and individuals who may try to take advantage of the war against Ukraine. Member States and operational partners are actively sharing relevant available information and criminal intelligence with Europol, which cross-checks and analyses the information and turns it into actionable operational intelligence notifications, such as early warning notifications and threat assessments, which are shared with partners.

Organised crime

Organised crime is already finding ways to exploit the current situation. Initial intelligence analysis identified crime patterns in a number of areas including human trafficking, false declarations of goods imported and exported, online fraud, cybercrime and firearms trafficking. There is also evidence of cybercriminals posing as fundraisers for Ukraine to steal

[26] COM(2022) 301.

money and cryptocurrency[27]. Criminal organisations from Ukraine may try to relocate due to the current situation and pursue their activities in the EU.

The Commission and the French Presidency of the Council worked together, as well as with the EU JHA Agencies, notably Europol, to mobilise the European Multidisciplinary Platform Against Criminal Threats (**EMPACT**), to assess, anticipate, prevent and counter existing or emerging serious and organised crime threats. On 7 April 2022, Europol hosted an EMPACT meeting gathering representatives and experts from the EU Member States and the EU security community to focus on threats of serious and organised crime which have emerged as a result of the war in Ukraine. Concrete steps discussed included the gathering of more intelligence, the implementation of emergency operational actions, and the refocussing of existing ones, as well as ad hoc joint action days.

CELBET (Customs Eastern and South-Eastern Land Border Expert Team) – a collaboration project financed by the European Commission, is following developments at the border as part of its mission to provide operational support and guidance to the customs officers and is monitoring the customs seizures at the border crossing points at the EU border (Poland, Slovakia, Hungary and Romania) with Ukraine.

Criminal and terrorist activity

Although no immediate terrorist threat has yet arisen in the EU in relation to the Russian invasion of Ukraine, the need for vigilance is clear.

The heightened risks of criminal and terrorist activity underline the importance for Member States to make use of relevant EU databases such as the Schengen Information System, to enter data there when necessary, and to consult them during checks on persons entering the EU. This will help to ensure that individuals who pose a threat to the internal security of the EU are identified at the external borders. EU-LISA, the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, continues to ensure the full availability and efficiency of the EU's border management systems. Guidance[28] to Member States has clarified how to balance the need to ensure smooth handling of arrivals at the external border while still performing the necessary security checks.

Preparedness

In addition to guidance and coordination, the EU's preparedness has been strengthened through the deployment of the EU agencies' staff.

Europol has deployed operational teams to the EU Member States neighbouring Ukraine. Those teams comprised of Europol guest officers from Member States and Europol experts in

[27] Google's Threat Analysis Group observed a growing number of threat actors using the war in Ukraine as a lure in phishing and malware campaigns. Researchers at internet security company Cyren report an increase in crypto scams taking advantage of the conflict through the use of fake donation websites.

[28] Commission Communication Providing operational guidelines for external border management to facilitate border crossings at the EU-Ukraine borders 2022/C 104 I/01.

Hungary, Lithuania, Poland, Romania, and Slovakia as well as Moldova[29]. Europol guest officers support the national authorities with Second-line Security Checks at the EU external borders. Europol experts provide support by collecting and assessing information to detect terrorist and criminal threats, to support investigations, and to identify individuals posing a risk by trying to enter the EU. These operational teams gather information which feed into criminal threat assessments available to Member States. Such intelligence gathering activity allows Europol to anticipate developments and coordinate operational activities with EU Member States to respond to the activities of criminal groups seeking to take advantage the war in Ukraine, and to build on Europol's active engagement with Ukrainian law enforcement through the Ukrainian liaison officer present at Europol's headquarters in the Netherlands.

The **European Border and Coast Guard Agency** (**Frontex**) is also present in Member States and EU neighbouring countries to support border control operations: more than 2100 border guards are currently deployed throughout the EU, in Western Balkan and in Moldova. **The European Asylum Support Office (EUAA)** has deployed almost 750 staff members in southern EU Members States and in Lithuania to support operational activities, reinforce reception capacities and help with asylum procedures.

Building on the current **Prüm Decision**[30], which provides a framework for Member States to deploy law enforcement officers for joint operations such as joint patrols, the Commission and the French Presidency of the Council of the European Union sent a joint letter to all Member States to identify needs, and requesting deployment of police officers, in order to launch joint patrols in the EU frontline Member States most affected by mass border crossings arising from the war. The Commission will finance these deployments under the Internal Security Fund/police.

Addressing trafficking in human beings

The EU has been on the alert from the first days of the war as to the risks of one particular area of criminal activity that might benefit from the huge movements of people seeking safety in the EU. It has been essential to prevent human traffickers targeting vulnerable people on the move, who are mostly **women and children,** using, for example, false offers of transport or lodging.

In March, Europol and Eurojust issued Early Warning notifications to relevant national authorities on potential trafficking in human beings and the exploitation of victims arriving from Ukraine. Eurojust helps enhance the exchange of information and speed up judicial cooperation including with Ukraine, and human trafficking investigations have been referred to the agency for coordination.

The EU Anti-trafficking Coordinator has held meetings with the EU Network of National Rapporteurs and Equivalent Mechanisms, the Justice and Home Affairs Agencies and the EU Civil Society Platform against Trafficking in Human Beings to exchange on the actions

[29] As of 3 May, Europol has deployed 1 Europol staff and 3 Guest Officers in Slovakia, 1 Europol officer in Poland, 1 Europol officer and 4 Guest Officers in Romania, and 2 Guest Officers in Hungary. 1 Europol staff and 2 Guest Officers are deployed to Moldova.

[30] 2008/615/JHA, 2008/616/JHA.

needed to prevent and combat abuses and protect victims. Investigations have been opened in several Member states on potential cases.

The EU has been swift and energetic in ensuring a coordinated response to this real threat to people that need the EU's help. Operational guidelines[31], including on the challenge of trafficking in human beings, were quickly offered to Member States implementing the Temporary Protection Directive to support those fleeing war in Ukraine. As part of the 10-Point Plan for stronger European coordination on welcoming people fleeing the war from Ukraine[32], presented at the Justice and Home Affairs Council on 28 March 2022, a Common Anti-Trafficking Plan[33] on preventing human trafficking and helping victims, has been developed by the EU Anti-Trafficking Coordinator, in cooperation with the EU Agencies and the Member states. Registering entities and individuals (including volunteers) that intend to provide accommodation, transport and other types of assistance, as well as performing background checks, is a particular focus. The Commission has also liaised with the EUAA to support detection of victims of human trafficking when health assessments are provided in reception centres. Unaccompanied or separated children are at particular risk of abuse, sexual exploitation or forced criminality. The above-mentioned Operational Guidelines also provide guidance to help Member States handling the arrival, reception and support to children, and unaccompanied minors in particular. In order to raise awareness among those at risk, the Commission has also launched a dedicated website with a section including practical advice on how to avoid traffickers.

While some actions to step up preparedness have been taken specifically in response to the new conditions arising from the war, other key measures flow from **legislative initiatives** already in the pipeline before Russia's war of aggression against Ukraine.

The Commission welcomes the agreement in February 2022 on the revised **Europol** mandate[34], which, once implemented, will allow Europol to better support Member States in the fight against organised crime and terrorism. The agency will then have the right tools and safeguards to support police forces in analysing big data to investigate crime and in developing pioneering methods to tackle cybercrime. These changes come with a reinforced data protection framework as well as stronger parliamentary oversight and accountability.

The package on **police cooperation** presented by the Commission on 8 December 2021[35] and currently being negotiated, will reinforce cooperation between law enforcement officials across Member States by making the exchange of data faster, easier, and more secure, as well as by enhancing and making more efficient operational police cooperation on the ground. The Commission calls on the European Parliament and the Council to quickly adopt this package.

Once adopted and implemented these legislative proposals will support law enforcement in the fight against cross-border organised crime. This will be particularly important in a context

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - EN - EUR-Lex (europa.eu).
[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en
[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en
[34] COM/2020/796.
[35] COM/2021/780, COM/2021/782, COM/2021/784.

where criminal organisations from Ukraine may try to relocate due to the current situation and pursue their activities in the EU.

The **EU Advisory Mission in Ukraine** has been supporting the reform of law enforcement and rule of law institutions in the country since 2014. In March 2022, the Mission's mandate was revised enabling support at the Ukrainian border crossing points with Poland, Romania and Slovakia, contributing to situational awareness on cross-border criminal activities including trafficking of human beings, and the flow of humanitarian goods into Ukraine.

IV. WEAPONS, DANGEROUS MATERIALS AND CRITICAL INCIDENTS

The war has massively increased the circulation of firearms and other weapons within Ukraine itself, which poses new risks for the EU and other states neighbouring Ukraine.

Vigilance and coordination

The operational guidance issued in March provided Member States with advice on how to tackle the challenge of increased circulation of firearms at a time of mass arrivals at the EU external border[36]. These guidelines underline that the presence of firearms should be continuously checked and that no one without authorisation should be allowed to enter the EU with a firearm. When any of these firearms are reported by Ukraine´s authorities as missing, the Member States should report them in the Schengen Information System.

It is crucial that all firearms shipments to Ukraine are properly recorded, with all relevant information (including type, country and year of manufacture, brand, make, caliber, serial number) in order to facilitate the traceability of those firearms, both in Ukraine and in the EU.

The EU has publicly deplored Russia's reckless military attacks at and in the direct vicinity of civilian nuclear, biological and chemical facilities in Ukraine, and any acts compromising the safety of these facilities. The Commission monitors the situation in Ukraine, paying particular attention to the radiological threat which is of the highest concern from the EU internal security point of view[37]. The Commission also monitors potential chemical threats, and has set up an internal coordination mechanism in case rapid risk assessment is needed.

Preparedness

Ukraine is already one of the countries identified as key for specific actions at external level in the EU Action Plan on Firearms Trafficking 2020-2025. There is also a specific operational action in the region including Ukraine, within the framework of EMPACT firearms. However, given the risks of firearms being diverted, specific EU-funded projects will be needed as well as operational cooperation with Europol, Frontex and the EMPACT firearms strand. The Commission will soon put forward a proposal to revise the Firearms Regulation[38] on exports, imports and transit of civilian firearms, as part of the overall legal and operational framework to prevent, detect, investigate and prosecute firearms trafficking.

---

[36] Commission Communication Providing operational guidelines for external border management to facilitate border crossings at the EU-Ukraine borders 2022/C 104 I/01.

[37] The Commission will organise – in cooperation with the US partners – a workshop focusing on the risks related to radiological materials located in hospitals going out of regulatory control.

[38] Regulation (EU) No 258/2012 of the European Parliament and of the Council of 14 March 2012

To improve the EU's preparedness and response to public health risks such as CBRN threats, the Commission is building up strategic reserves of response capacities through the EU Civil Protection Mechanism (UCPM), funded by the Health Emergency Preparedness and Response Authority (HERA)[39]. The Commission services are working together on developing a €540.5 million rescEU strategic stockpile. This stockpile will consist of equipment and medicines, vaccines and other therapeutics to treat patients exposed to CBRN emergencies agents, as well as of rescEU decontamination reserve to provide decontamination equipment and expert response teams. As an immediate first step, the EU has mobilised its rescEU medical reserve to procure potassium iodine tablets which can be used to protect people from the harmful effects of radiation, as well as other items urgently needed in Ukraine. Already almost 3 million iodide tablets have been delivered to Ukraine via the UCPM, with the help of France and Spain.

V. COORDINATED ACTION TO BRING RUSSIAN AGGRESSION TO ACCOUNT

The EU is playing a decisive role in the actions of the international community to put pressure on Russia to end its aggression against the Ukrainian state and civilians caught up in the conflict, which is unacceptable and contrary to international law. This pressure includes measures to indicate the consequences for the perpetrators including severe sanctions, and actions to identify and facilitate prosecution of war crimes.

Restrictive measures and confiscation

Since Russia's recognition of the non-government-controlled areas of the Donetsk and Luhansk oblasts in Ukraine on 21 February 2022, and the invasion of Ukraine on 24 February 2022, the EU has imposed the largest ever series of restrictive measures against Russia. So far, five sanction packages have been adopted. These measures focus on key sectors, including finance, trade, transport, defence, and media and target political and military elites as well as prominent Russian and Belorussian oligarchs. Listings already include more than 1000 individuals and 80 entities. A sixth package of sanctions is under discussion in the Council.

The impact of these and previous restrictive measures against Russian and Belorussian individuals and companies will be as strong as their enforcement. EU coordination can make a major contribution to closing potential loopholes, and the Commission has provided extensive support to stakeholders, through written guidance, meetings of stakeholders and a dedicated expert group, and a range of resources to facilitate compliance.

In addition, the Commission has set up a 'Freeze and Seize' Task Force bringing together Commission services, Member States, Eurojust and Europol. So far, Member States reported to have frozen assets worth €9.89 billion[40]. On 11 April, Europol, jointly with Member States, Eurojust and Frontex, launched Operation Oscar to support financial and criminal

implementing Article 10 of the United Nations' Protocol against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition, supplementing the United Nations Convention against Transnational Organised Crime (UN Firearms Protocol), and establishing export authorisation, and import and transit measures for firearms, their parts and components and ammunition.

39 HERA Work Plan 2022 (europa.eu)

40 There is also an amount of blocked assets of the Russian Central Bank of approximately €23 billion.

investigations targeting criminal assets owned by individuals and legal entities covered by EU sanctions related to Russia's war against of Ukraine. The EU's Freeze and Seize Task Force works closely alongside the 'Russian Elites, Proxies, and Oligarchs (REPO)' Task Force, set up by G7 countries (Canada, France, Germany, Italy, Japan, the United Kingdom, the United States) and like-minded partners such as Australia as well as the US KleptoCapture Task Force and the Ukrainian Task Force.

The 'Freeze and Seize' Task Force serves as a platform to coordinate and facilitate the exchange of information and experience across Member States and to provide guidance on the implementation of sanctions, and to facilitate the exchange of best practice on criminal investigations and confiscation. In particular, it is important that law enforcement authorities are alert and proactive in relation to potential crimes by the sanctioned individuals and entities. The Task Force also aims to bring forward discussions on possible deployment of confiscated funds, for example to contribute to the reconstruction of Ukraine.

The Commission is today adopting an **asset recovery and confiscation** package[41], which takes into account the lessons learned from the implementation of Union restrictive measures against Russian and Belorussian individuals and entities. It will facilitate the effective implementation of EU Union restrictive measures across the Union by enabling the swift tracing and identification of property owned or controlled by persons or entities subject to such measures. The enhanced asset recovery and confiscation framework will also apply to the violation of restrictive measures and will thus ensure the effective tracing, freezing, management and confiscation of proceeds derived from the violation of restrictive measures. To ensure that the assets of the individuals and entities that violate the restrictive measures can actually be confiscated, the Commission is also adopting today proposals for a Council decision to add the violation of sanctions to the list of EU crimes in Article 83(1) TFEU[42] accompanied by a Communication[43], with a view to proposing a Directive to approximate the definition of criminal offences and penalties for the violations of restrictive measures.

In a more general way this package marks a crucial step in the fight against organised crime. It follows the Commission's commitments made in the Security Union Strategy and the Strategy to tackle Organised Crime 2020-2025[44]. It revises the 2014 Confiscation Directive, the 2007 Council Decision on Asset Recovery Offices (ARO), and the 2005 Framework Decision Confiscation of Crime-Related Proceeds, Instrumentalities and Property to strengthen capabilities in tracing and identification and ultimately confiscating illicit gains addressing the very low rates of confiscation in the EU[45]. The package expands the scope of criminal offences covered and extends rules on confiscation in cases where a criminal conviction for a specific crime is not possible but where the assets clearly stem from criminal activities. The revision also strengthens effective management of frozen and confiscated assets and reinforces the capacity of AROs to trace and identify illicit assets. The new EU asset recovery framework is designed to address the complex modus operandi of criminal organisations, which frequently operate across borders and use different methods to conceal their assets, including by means of crypto assets.

---

41 COM(2022) 245.
42 COM(2022) 247.
43 COM(2022)249.
44 COM(2021) 170.
45 Europol estimates that only 2% of criminal assets are frozen (€2.4 billion) and 1% confiscated (€1.2 billion), while criminal revenues in the main criminal markets in the EU amounted to €139 billion in 2019 (1% of the EU GDP).

Coordinated judicial response

Work has also been ongoing at EU level to ensure a coordinated judicial response to **international crimes** allegedly committed in Ukraine, so that perpetrators can be held to account.

A Joint Investigation Team (JIT) was set up by two Member States and Ukraine to investigate war crimes, crimes against humanity and other international crimes allegedly committed on Ukrainian territory. Eurojust provides legal, analytical, financial and logistical support to this JIT. On 25 April 2022, the Office of the Prosecutor of the International Criminal Court (OTP-ICC) joined the JIT as participant[46] and additional participants are expected to join soon.

On 25 April 2022, the Commission presented a proposal to amend the Eurojust Regulation[47] in order for Eurojust to preserve, analyse and store evidence of core international crimes. Eurojust and Europol will continue to work closely together throughout this process. A crucial role in coordinating the judicial response is also played by the Genocide Network, of which Eurojust hosts the Secretariat, which has prepared an Atlas of NGOs currently active in Ukraine and supports national practitioners from Member States and Ukraine handling active cases related to the war.

In April 2022, the Council further revised the mandate of the **EU Advisory Mission in Ukraine**, paving the way for Mission's support to Ukrainian authorities in the investigation and prosecution of any international crimes committed in the context of Russia's military aggression. The Mission will provide Ukrainian authorities with strategic advice on the investigation and prosecution of international crimes, necessary amendments to Ukrainian legislation, communication strategy, as well as training on related matters. The Mission is part of a number of coordination initiatives in this context and, jointly with the EU Delegation, is part of the US-EU Atrocity Crime Advisory Group of Ukraine.

VI. FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

Current geopolitical developments have underlined the risks of foreign interference. Russia's military aggression against Ukraine has been accompanied by information **manipulation and interference** activities. Baseless allegations of 'Nazism' and 'genocide' against the Ukrainian government, false flag operations and unfounded accusations against NATO and the West have been deployed to justify brutal attacks on Ukraine, while free speech and independent reporting inside Russia have been suppressed. There is a continuing risk from manipulated audio-visual material and disinformation that Russia may attempt to use as a pretext for additional military attacks, to weaken the resolve of the Ukrainian resistance, to divide the international community in its opposition to the war, or to sow doubts about Russia's breaches of international law. The EU committed in the Strategic Compass to firmly respond to foreign information manipulation and interference and enhance its resilience and ability to counter such threats.[48] Manipulation of the democratic debate inside the EU is the

[46] https://www.eurojust.europa.eu/eurojust-and-the-_war-in-ukraine
[47] COM(2022) 187 final.
[48] https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

subject of the European Democracy Action Plan, the Commission's coordinated plan to address disinformation and strengthen democratic resilience[49].

Vigilance and coordination

The European Union responded through decisive and coordinated action to Russia's disinformation campaign in the context of the military aggression against Ukraine. The EU has worked closely with its Member States via the Rapid Alert System, and with international partners such as NATO, the US, Canada and the G7 Rapid Response Mechanism, to share insights into the manipulation trends and tactics employed by the Kremlin. Work to deconstruct the Kremlin's manipulations has intensified, notably via the EUvsDisinfo website, which broadcasts in English, Russian, Ukrainian and other languages, to provide factual information inside the EU, in Ukraine and the region, as well as inside Russia. Since 2 March, transmission and broadcasting of Russian State media RT and Sputnik channels in the EU or directed at the EU was suspended, as a consequence of restrictive measures adopted by the EU. Online platforms, leading social networks, advertisers and advertising industry signatories of the Code of Practice on Disinformation[50] are taking urgent action to limit disinformation related to Russian aggression of Ukraine. The Commission and the EEAS are monitoring these efforts. The information provided shows that platforms have strengthened their monitoring and intervention tools related to the war.

In addition, actions are rapidly being rolled out to support countries in Central Asia and the Western Balkans to strengthen information resilience and counter foreign information manipulation and disinformation.

Preparedness

The overt use of foreign information manipulation and interference (FIMI), including disinformation as one of the tools of hybrid threats, has brought extra urgency to the follow-up of the European Democracy Action Plan. Over recent months, the EU institutions have supported Member States in countering FIMI, especially in the framework of the Rapid Alert System by sharing insights on the tactics used by FIMI actors and on response strategies. Discussions to further reinforce the EU's overall response to FIMI, are ongoing, on the basis of a concept note presented by the EEAS on developing a dedicated **Toolbox** to address this threat. This brings existing internal measures and new EU tools under the common foreign and security policy together. It will also benefit from the intensified action of the European External Action Service Stratcom[51] as well as the Commission.

The European Digital Media Observatory ('EDMO') established a task force on disinformation following the outbreak of war in Ukraine and coordinates actions by fact-checkers and researchers in its network. It has analysed how COVID-19 conspiracy theorists

[49] COM(2020) 790.

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[51] The Strategic Communication, Task Forces and Information Analysis Division of the European External Action Service provides strategic communication support in the implementation of EU foreign and security policy in related priority regions (Southern and Eastern Neighbourhood, the Western Balkans) by developing and implementing specific strategic communication actions focused on advancing EU policies, values, objectives and interests.

have swiftly pivoted towards disseminating pro-Russian hoaxes, a shift observed in a number of Member States[52].

The Digital Services Act proposal seeks to adapt to rapidly evolving digital technologies and what this means for technological and democratic challenges, such as hate speech, disinformation online and destabilisation strategies. Significant progress in the negotiations by the European Parliament and the Council should allow for swift adoption of the package.

VII. BROADER PREPAREDNESS

At a time when war has returned to Europe, as well as a time of major geopolitical shifts, security coordination in the EU has moved up a gear, drawing on initiatives already in the pipeline before Russia's war of aggression against of Ukraine. Initiatives looking primarily to the EU's external security have powerful implications for the internal agenda of the Security Union.

On 15 February 2022, the Commission put forward the **Defence package**[53], with a number of initiatives in areas critical for defence and security within the EU. This contribution of the Commission to European defence and security covers the full range of challenges. It proposes concrete steps towards a more integrated and competitive European defence market, particularly by enhancing cooperation within the EU and building economies of scale. It also entails a roadmap on critical technologies for security and defence to boost research, technological development and innovation in these sectors and reduce dependencies in critical technologies and value chains. The package also aims at strengthening the defence dimension of space at EU level. In addition, it looks into how the Commission could step up its actions against hybrid threats, including in the cyber domain, enhance military mobility within and beyond Europe, and further address climate change challenges related to defence. To complement this work, the Joint Communication **'Defence Investment Gaps Analysis and way forward'**[54] of 18 May considers the capability and industrial gaps that need to be addressed with a view to support most exposed EU Member States and identify measures to mitigate the identified shortfalls.

The EU's resilience to these threats also implies capability-driven approaches across security sectors, as advocated in the Commission Action Plan on synergies between civil, defence and space industries[55]. Work is ongoing to promote capability-driven approaches in the field of internal security and law enforcement.

On 21 March 2022, the Council adopted the **Strategic Compass for Security and Defence**[56], endorsed shortly afterwards by the European Council. The Compass outlines an ambitious plan of action for strengthening the EU's security and defence policy by 2030. The objective

---

52 https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/

53 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en

54 JOIN(2022)24.

55 COM(2021)70.

56 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: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

is to make the EU a stronger and more capable security provider, which protects its citizens and contributes to international peace and security. It contains concrete proposals, with a very precise timetable for implementation, to improve the EU's ability to act decisively in crises.

One of the deliverables of the Strategic Compass is the development of an **EU hybrid toolbox** that should provide a framework for a coordinated response to hybrid campaigns affecting the EU and its Member States, including internal and external measures. Following the identification of sectoral resilience baselines carried out at the beginning of 2022[57], an analysis of gaps and needs will be completed. It is in this framework that the EU will continue to build preparedness, resilience and response to threats arising from Russia's aggression and any other attempts to destabilise democracies and the rules-based multilateral order.

VIII. LOOKING AHEAD

Looking ahead, the EU will need to remain extremely vigilant to evolving threats, and build **preparedness and resilience to all eventualities**. The repercussions of the war may take different forms, not all of which can yet be assessed.

The extent of displacement of Ukrainian criminal networks is not yet known. Eurojust's past casework indicates a trend of trafficking of heroin from Afghanistan to the EU via Ukraine, as corroborated by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)[58]. Instability may make it more difficult to act against the heroin trade via this route, bringing the risk of a possible increase in the flow of drugs to the EU.

Some risks to the EU are more likely to grow at the end or during potential pauses in the fighting. Particular attention will be paid to the the circulation of firearms, with the risk increasing when fighting in Ukraine subsides. Past experience also points to the risk that the return of foreign fighters who have gained combat experience and who may have come into contact with extremist groups, may bring terrorist action to the EU at a later stage. This potential phenomenon should be carefully monitored, and the Commission is already facilitating discussions among Member States on the challenges raised by the return of foreign volunteers with violent extremist background.

In view of these possible threats, it is important that the implementation of the Security Union Strategy continues, including with the implementation of key strategies such as the EU Cybersecurity Strategy, the Strategy to tackle Organised Crime (2020-2025), Counter-Terrorism Agenda for the EU (2020-2025), the EU action plan on firearms trafficking (2020-2025), the EU Strategy on Combatting Trafficking in Human Beings (2021-2025), and the EU Drug strategy (2021-2025).

---

[57] SWD(2022) 21 final.

[58] Report on the drug and alcoholic situation in Ukraine for 2020 (according to 2019 data), OEDT, Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery, 2021/00446, Eurojust, May 2020.

Efforts to provide the EU with the necessary legislative framework will continue. For example the Commission is preparing the impact assessment for a proposal regulating the marketing and use of high-risk chemicals.

IX. CONCLUSION

The Security Union continues to play its role in preparing the EU and its Member States to tackle existing and potential threats. Russia's war of aggression against of Ukraine has shown how quickly theoretical threats can become real, and underlines the importance of vigilance, coordination, and preparedness.

This fourth progress report on the Security Union Strategy demonstrates that the EU is able to adapt, even in the face of exceptional and unexpected threats such as from Russia's war of aggression against Ukraine. Determined implementation of the Security Union Strategy is more important than ever.