Council of the
European Union

Brussels, 30 June 2022
(OR. en)

10601/22

LIMITE

JAI 943
COSI 183
CRIMORG 98
ENFOPOL 373

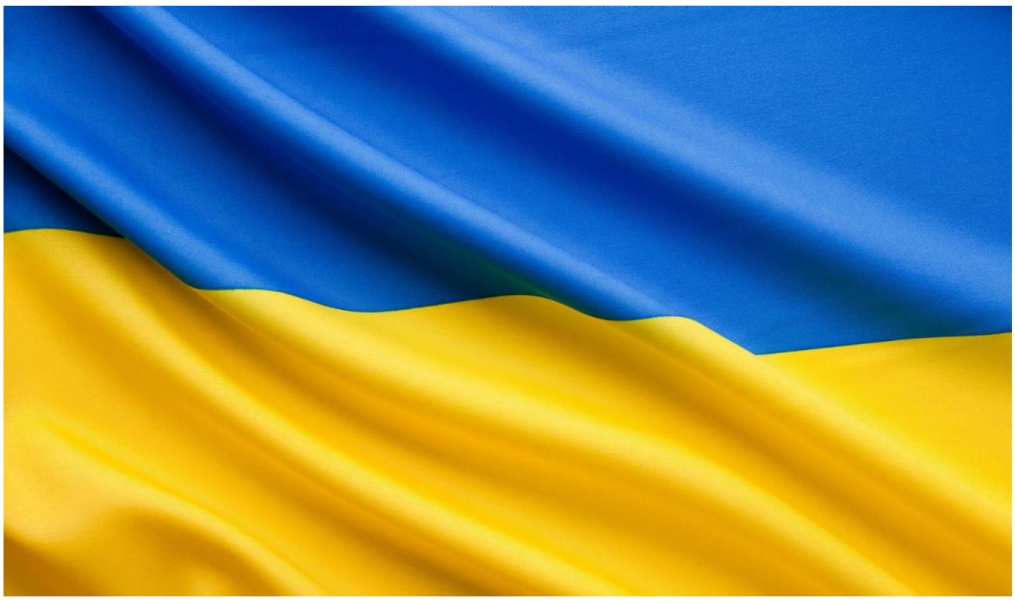
NOTE

From:	Europol
To:	Delegations
Subject:	Impact of the Russian war of aggression against Ukraine on crime and terrorism in the EU - Follow-up assessment June 2022

Delegations find enclosed Europol's threat assessment on the "Impact of the Russion war of aggression against Ukraine on crime and terrorism in the EU".

Impact of the Russian war of aggression against Ukraine on crime and terrorism in the EU

Follow-up assessment June 2022



The Hague,

Ref. no 2022-93,
30/06/2022

Contents

Key findings

- **Criminal networks have once more demonstrated their flexibility and adaptability during the Russian war of aggression against Ukraine.** Criminal activity has continued despite the logistical challenges presented by the war for crime areas like firearms smuggling, excise fraud and to a lesser extent, vehicle trafficking.
- **As the war in Ukraine enters into a new phase, the situation on the ground changes also with respect to the criminal threats to the EU**. With the theatre of combat operations moving eastwards, some previously disrupted criminal activities are likely to resume, such as local drugs trafficking.
- **Criminal networks acted on emerging opportunities for crime presented by the war. A number of on-going criminal investigations highlight the immediate and short-term impact of crime.**
  - **Weapons** continued to be detected in possession of individuals trying to leave Ukraine and several investigations have been opened into criminal networks smuggling weapons from the battlefield to the EU.
  - The **misuse of Ukrainian documents**, genuine or fraudulent ones, has been increasingly reported in relation to migrant smuggling of non-Ukrainian nationals.
  - The number of reported **cyber-attacks** on EU targets has steadily increased. While the impact of these attacks has remained limited so far, EU critical infrastructure is also considered a target and therefore future cyber-attacks may result in more severe disruption.
- **For some criminal activities, the short-term impact appears to be limited. However, these threats may materialise on medium- to long-term.**
  - The **trafficking in human beings, particularly for sexual exploitation,** targeting Ukrainian refugees remains a risk. However, the number of confirmed cases so far has remained limited. It is nonetheless likely that more cases will surface, also with regard to labour exploitation and child trafficking, over the duration of the conflict and in its aftermath.
  - In addition to potential money laundering activities related to **Russian individuals subjected to EU sanctions**, **some cash seizures** have been made from Ukrainian refugees entering the EU. However, money laundering is challenging to confirm since the illicit origin of the money cannot be established with the information available.
  - **Disinformation** campaigns continue, using social media platforms to address a wider and a more diverse public, including in the EU. Disinformation has the potential to further erode EU communities' trust in the ability of authorities to tackle the crisis and may also enforce violent behaviours and narratives.
  - Clear indications of a geographic displacement of **Russian-speaking criminal networks** are currently limited but are closely monitored. The business of Ukrainian migrant smugglers into and within the EU, as known before the war, has continued. Ukrainian criminal networks may also become more involved in the exploitation of Ukrainian refugees.
  - **There are limited indications of potential terrorist threats emerging from or in relation to the war in Ukraine.** Nonetheless, particularly right-wing groups and supporters have reacted in the online environment with propaganda, calls for mobilisation, travel planning or financing campaigns.

Introduction

Since the start of Russia's illegal invasion of Ukraine on 24 February 2022, Europol has been closely monitoring the impact on serious and organised crime and terrorism in the EU.

Regular Monitoring Reports are shared with EU Member States and partners, which present developments in serious and organised crime and terrorism linked to the Russian war of aggression against Ukraine. In addition, specific assessments have been produced focusing on firearms trafficking and trafficking in human beings. In March 2022, Europol issued a Preliminary Assessment and a Follow-up Assessment looking into serious and organised crime and terrorism assessing the most pressing threats to the EU.

Scope and focus

This report provides an assessment of the potential impact of the Russian war of aggression against Ukraine on crime and terrorism in the EU. The current intelligence picture and an identification of the key threats in the short-, mid- and long-term perspective provide a basis for the formulation of areas to target for operational (preventive or reactive) activities.

The report is based on information supplied to Europol by Member States, partner countries and agencies, as well as the monitoring of sources by various teams at Europol covering the mandate of the agency. Europol is in close contact with Member State authorities and its partners to continuously exchange information on the current situational picture and developments.

The report assesses potential changes in the key threats for the EU stemming from the Russian war of aggression against Ukraine, identified in previous reports. For this purpose, on the occasion of the second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine that took place on 9 June 2022, the preliminary findings were presented and a request to further contribute with information has been launched to EU Member States, partner agencies and operational partner countries.

This intelligence-led approach aims to ensure the most pressing current and emerging threats are addressed as priorities when operational initiatives are planned.

Caveat

Information on and from areas of armed conflict is often unreliable. The deployment of methods of hybrid warfare and the widespread deliberate use of disinformation further obscure the intelligence picture. The assessment presented here is based on information assessed as relevant and reliable at the time, but may change as further or different information becomes available.

Background

As the Russian war of aggression against Ukraine continues, it is estimated that since 24 February 2022, more than 7.7 million border crossings from Ukraine have been reported to neighbouring countries and over 5 million individual refugees from Ukraine have been recorded throughout Europe. The main EU Member States of first entry have been Poland, Romania, Hungary and Slovakia. Over 3.4 million refugees from Ukraine registered for Temporary Protection or similar national protection schemes in Europe.

2.5 million border crossings to Ukraine were also reported.[1] The main reasons for which refugees return to Ukraine, as reported by UNHCR, are reunification with the family, perception of safety in the area of return, temporary visits to get supplies or to visit family members, difficulties in finding housing in neighbouring

[1] UNHCR, accessible at https://data.unhcr.org/en/situations/ukraine, updated 16 June 2022

countries and supporting family members to evacuate. Nonetheless, it is expected that the return trend will not become a stable development, but rather a cyclical or temporary one. [2]

As of June 2022, the number of cross-border investigations directly related to the war in Ukraine has remained at low levels, with few confirmed cases concerning serious and organised crime and terrorist activities. However, given the high adaptability of criminal networks constantly trying to exploit opportunities, the risks emanating from serious and organised crime substantiate the need to continue information sharing and the active monitoring of all crime areas where changes may be prompted by the situation in Ukraine.

The impact of the war may take the form of geographical shifts and displacement of crime in the EU, as well as that of changes in the volume and typology of particular types of crimes committed by EU-based criminals.

Information contributed to Europol

EU Member States and partner countries have contributed information to Europol, in order to generate a more accurate intelligence picture on potential developments in serious and organised crime that may be connected to the Russian war of aggression against Ukraine. Most of the information contributed since 24 February concerned trafficking in human beings, asset recovery, migrant smuggling, trafficking in weapons and explosives, as well as fraud, excise fraud, money laundering and cybercrime. [3]

The information shared in relation to the war in Ukraine revealed links with entities in Europol's databases reported before and after 24 February 2022 in connection to crime areas such as migrant smuggling, excise fraud, Eastern European organised crime, money laundering, trafficking of weapons and explosives, asset recovery, property crime, THB, trafficking of cocaine and synthetic drugs, cybercrime etc.

In the area of counter-terrorism, most contributions related to core international crimes, suspicious individuals relevant for non-Islamist extremism reportedly fighting in Ukraine and requests for detention and provisional arrests of suspects received from Ukrainian authorities.[4]

Impact on serious and organised crime and terrorism in the EU

Russian-speaking criminal networks

The threat of a displacement of Russian-speaking criminal networks remains, and indications of their establishment, activities, and use of corruption, money laundering, violence and misuse of legal business structures are closely monitored, but have not yet emerged.

Russian-speaking criminal actors have long been active in the EU. Among other crimes, Russian criminal networks, some including members of the prolific Thieves-in-Law (vory-v-zakone), have been operating complex money laundering schemes, often using legal business structures and have infiltrated EU's legal economy using corruption. Belarusian criminals have been well known for dealing with excise fraud involving illicit tobacco products and alcohol smuggled from Belarus to the EU, as well as migrant smuggling. Ukrainian criminal networks operating in the EU have specialised in cybercrime, migrant smuggling, tobacco smuggling, organised property crime, investment fraud and money laundering, among others.

[2] UNHCR, Border crossings to Ukraine (since 28 February 2022), accessible at https://data.unhcr.org/en/situations/ukraine
[3] Information extracted for the period between 24.02.2022 and 21.06.2022
[4] Information extracted for the period between 24.02.2022 and 21.06.2022

Chechen criminals and groups have been visible in the EU's serious and organised crime landscape over the past years for their involvement in extortion, drug trafficking and migrant smuggling. They have also been noted for their violent clashes with other criminal groups.[5]

Russian-speaking criminals are very likely to target Ukrainian victims for trafficking in human beings. For instance, they have been observed near reception centres in European countries attempting to offer Ukrainian nationals money or housing in exchange of documents received that allow them to work in the receiving country. In addition, instances of known Thieves-in-Law leaving Ukraine after the beginning of the war have also been reported in the EU.[6]

Europol has received information that new criminal groups have been detected in the EU after 24 February, including Russian-speaking criminal networks.[7] Moreover, investigations are ongoing in Member States into activities of Russian-speaking networks, including some concerning Thieves-in-Law.[8]

Threat assessment and way forward

The war in Ukraine, EU sanctions and the degrading economic situation in their origin countries may drive Russian-speaking criminal networks and high-ranking criminals to relocate their operations to the EU.

Similarly, new criminal opportunities may emerge, such as money laundering delivered as a service to Russian individuals, the supply of commodities (potentially counterfeit) needed on the war front in Ukraine or becoming increasingly scarce in Ukraine and Russia, due to the economic downturn both countries are experiencing. Firearms trafficking may also become an attractive venture, given the availability of weapons in Ukraine and the potential utilisation of routes and infrastructure used in the past to smuggle commodities out of the affected countries.

EU-based Russian-speaking criminal networks may similarly take advantage of the inflow of Russian-speaking refugees coming to the EU, for exploitation or to recruit collaborators in their criminal operations, through community connections and common language.

Developments in Ukraine might also trigger violent confrontations between Russian-speaking criminal groups in the EU, as well as acts of extreme violence, as seen in the past for example in the case of Chechen groups. However, to the moment, no indications of such developments have been reported to Europol.

Firearms trafficking

In addition to indications of organised smuggling of weapons from Ukraine, several cases where individuals attempted to exit Ukraine carrying firearms have been reported. Moreover, concerns were voiced regarding weapon caches along the Ukrainian borders with the EU as a potential modus operandi to smuggle firearms to the EU.

After the beginning of the military aggression in Ukraine in 2014, groups and individuals looted some of the state-owned arms and ammunition storage facilities. It was estimated that by 2015, battlefield seizures and other forms of diversion led to 300 000 small arms and light weapons going missing. These events led to the widespread circulation of military-grade small arms and light weapons outside of state control, some

[5] Europol information
[6] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[7] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[8] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022

of which found their way into the hands of criminals. Moreover, weapons and ammunition sourced from eastern Ukraine were also regularly found for sale online. Despite the large quantities of illicit ammunition circulating in Ukraine after 2015, trafficking to neighbouring countries and elsewhere in Europe remained low, which may have been attributed to the law enforcement efforts but also, potentially, to continued demand for small firearms in the country.[9]

The Russian war of aggression against Ukraine has resulted in the proliferation of a significant number of firearms and explosives in the country and information was shared with Europol on both individuals trying to exit Ukraine carrying weapons and on more organised smuggling activities.

The individuals apprehended while attempting to exit Ukraine with weapons were EU nationals, as well as citizens from other countries in and outside of Europe. In most cases, the individuals detected declared that they had travelled to Ukraine as volunteers and that the weaponry found in their possession was either given by Ukrainian authorities or brought from their home countries.[10]

Several EU Member States receiving large numbers of refugees from Ukraine voiced concerns that some refugees have carried firearms for self-defence purposes, abandoning them at the border before crossing into the EU. Cases of ammunition allegedly abandoned on the Ukrainian side of border-crossing points with the EU were also reported.[11] Weapons and ammunition caches left behind in Ukraine may be collected by criminals.[12] There are indications that some criminals operating from Ukraine may be hiding firearms along the green border with the EU and then return via official border-crossing points to retrieve them from the EU-side of the green border.[13] Some refugees are suspected to bring concealed firearms across the border, which once in the EU can be sold on or exchanged for goods or services, including those of illicit nature.[14] In some cases, firearms were allegedly exchanged for services such as transportation offered by taxi drivers.[15]

In addition to instances where individuals were apprehended trying to move weapons outside of Ukraine, there are on-going cases supported by Europol indicating that more organised forms of trafficking activities may have already commenced. EU Member States and Operational Partners have reported cases of criminal networks active in the region engaging in or planning the smuggling of significant amounts of firearms and ammunition, including military weapons.[16]

According to information received by Europol, firearms are also being trafficked to Ukraine from the Western Balkan region.[17]

Threat assessment and way forward

[9] Small Arms Survey, March 2022, Footnotes: Takeaways from previous Small Arms Survey research on Ukraine, accessible at https://smallarmssurvey.medium.com/footnotes-takeaways-from-previous-small-arms-survey-research-on-ukraine-adff89b864d5
[10] Information contributed to Europol by EU MS and Operational Partners
[11] Europol information; Europol, April 2022, Potential firearms and explosives trafficking activities related to the Russian war of aggression against Ukraine, EU Unclassified, Basic Protection Level
[12] Europol, April 2022, Potential firearms and explosives trafficking activities related to the Russian war of aggression against Ukraine, EU Unclassified, Basic Protection Level
[13] Information contributed to Europol by EU MS
[14] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[15] Europol information; Europol, April 2022, Intelligence Notification on Potential firearms and explosives trafficking activities related to the Russian war of aggression against Ukraine, EU Unclassified, Basic Protection Level
[16] Europol information ; Information contributed to Europol by Operational Partner; Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[17] Information contributed to Europol by EU MS

In the short term, weapons and ammunition brought into the EU by individuals returning from the battlefield in Ukraine may be dispersed into EU black markets. Established routes previously used for migrant smuggling activities or the transportation of illicit commodities may be used for the trafficking weapons in the future, as well as online platforms where criminals may advertise and trade them. Traffickers will likely exploit the high quantities of weapons available in Ukraine, engaging in the trafficking of stolen, abandoned or lost firearms and ammunition.

Civilian drones are being used against Russian forces in Ukraine and, in some cases, they are technologically enhanced for example, to launch bombs and grenades or to carry anti-tank grenades. 3D printing is also allegedly used to increase the damage produced. Under these circumstances, there is a possibility, in the medium to long term, that such products may also be smuggled to the EU together with traditional weaponry.

On the mid- and long-term, Ukraine may emerge as a source of illegal firearms smuggled into the EU, given the significant expansion of potential supply and sustained demand for firearms by EU-based criminal networks. Countries neighbouring Ukraine are likely to become transit hubs for firearms trafficked from Ukraine to the EU, not only due to their geographical position but also due to the pre-existing criminal infrastructure active here.

Cybercrime

Cyber-attacks against EU targets appear to have intensified since April, with a limited impact. There are indications that attacks may increasingly target critical infrastructure in the EU.

Malicious cyber activities have emerged as one of the most apparent criminal activities linked to the war against Ukraine. Various threat actors are involved in these activities, which target Ukrainian, Russian and EU and Member State governmental entities, organisations, companies and individuals. In many cases, these activities involve the intrusion into systems to disrupt services, and/or exfiltrate and subsequently release data.

Ukrainian digital infrastructures and government websites have been targeted by DDoS attacks even before 24 February and cybercriminals have been targeting the Ukrainian government and officials with different malware variants, such as the IcedID malware, in order to compromise personal data or access information.[18] These attacks appear to have become more severe and the cybercriminals believed to be responsible for them are likely non-state and state-sponsored actors originating from Russia as well as Belarus.[19]

Russian digital infrastructure is also being targeted. A wave of data thefts and subsequent data leaks seems to have affected Russian public and private organisations. The transparency collective Distributed Denial of Secrets has published several datasets including personal data from Russia. These are often submitted by anonymous hackers, many of them self-identifying as part of the Anonymous collective, and then made available online.[20] According to open sources, a hacking group obtained and announced the upcoming release of personal information of more than 600 agents of the Russian Federal Security Service (FSB).[21]

[18] The Hacker News, April 2022, New Hacking Campaign Targeting Ukrainian Government with IcedID Malware, accessible at https://thehackernews.com/2022/04/new-hacking-campaign-targeting.html
[19] Information contributed to Europol by Operational Partner
[20] The Intercept, 22 April 2022, Russia is losing a war against hackers stealing huge amounts of data, accessible at https://theintercept.com/2022/04/22/russia-hackers-leaked-data-ukraine-war/
[21] Cybernews.com, March 2022, Hundreds of alleged Russian spies revealed in a data breach, accessible at https://cybernews.com/cyber-war/hundreds-of-alleged-russian-spies-revealed-in-a-data-breach/

Since April 2022, cyber-attacks have increased in frequency and scope. The vast majority of these cyber-attacks is believed to have been carried out by pro-Russian threat actors and targeted websites of entities, including websites of public authorities, causing very limited to no losses. The downtime of these services was low and the attacks were mitigated rapidly. Despite the sophistication and expertise of well-known cyber threat actors believed to be behind these activities, no major attacks compromising sensitive data or disruptions were reported. This might indicate that these actions are perpetrated to send a political message in response to the EU's economic, humanitarian and material support to Ukraine.

In some cases, digital infrastructure in the EU was targeted by criminals thought to be based in Russia. Targets included banks, telecommunication or transport providers, internet domains, websites of public authorities, individual entrepreneurs and companies. Phishing and crypto locker ransomware campaigns were carried out in the EU, not attributed but believed to be connected to Russian actors.[22]

The attribution of attacks is often difficult and not entirely reliable. In most cases, well known groups claim responsibility for the attacks on social media posts, showing support to one of the involved parties.

The Russian cybercrime group Killnet has recently emerged as a prominent threat actor in connection to cyber-attacks targeting the EU. A series of Distributed Denial of Service (DDoS) attacks aimed at disrupting national services was reported in several EU Member States. Killnet claimed responsibility on groups on instant messaging platforms.[23] Similar attacks carried out in the beginning of May on German[24] and Italian[25] institutions. More recently, the computer network of Germany's Greens, partners in the ruling coalition government, openly calling for Germany to send more weapons to Ukraine, has been hacked by yet unknown intruders.[26] Monitoring of instant messaging service channels has revealed that some threat actors may be planning attacks with a higher impact.[27]

Threat assessment and way forward

The risk of Member States, EU-based organisations and EU citizens being targeted by malicious cyber activities will likely remain high in the near future. In addition to Ukraine's digital infrastructure, EU institutions may continue to be targeted by those criminal actors supporting the Russian war, perpetrating cyber-attacks in response to the introduction of EU sanctions against Russia or in retaliation for the EU's support for Ukraine. These attacks might intensify both in volume and severity, potentially targeting critical infrastructure of EU Member States.

Migrant smuggling

The threat emanating from migrant smuggling in the context of the war in Ukraine remains low. However, the use of fraudulent Ukrainian documents for the smuggling of other nationalities

[22] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April; Europol, meeting with the Heads of Criminal Police from EU Member States and the Ukrainian Liaison Officer to Europol on Coordinated Law Enforcement Approach to Ukraine, 4 April 2022
[23] Information contributed to Europol by EU MS
[24] Der Spiegel, 06 May 2022, Cyberangriffe von Killnet - Putin-Fans attackieren deutsche Behördenseiten, accessible at https://www.spiegel.de/politik/deutschland/killnet-cyberangriffe-wladimir-putin-fans-attackieren-deutsche-behoerdenseiten-a-2be17f20-3688-4674-b82d-d7889a532c80
[25] Reuters, 11 May 2022, Pro-Russian hackers target Italy institutional websites -ANSA news agency, accessible at https://www.reuters.com/world/europe/pro-russian-hackers-target-italy-defence-ministry-senate-websites-ansa-news-2022-05-11/
[26] Reuters, 16 June 2022, Germany's hawkish Greens report computer system hack, accessible at https://www.reuters.com/article/germany-politics-cyber/germanys-hawkish-greens-report-computer-system-hack-idINL8N2Y33LD
[27] Europol information

into the EU appears to have increased and may become more prominent in other crime areas dealing with movement of people and commodities.

Migrant smuggling has not emerged as a major crime threat associated with the Russian war of aggression against Ukraine. In line with the temporary protection regime established by the EU, Ukrainians and third country nationals legally residing in Ukraine before the start of the conflict have the right to enter, travel, and work in the EU.

Smuggling of irregular migrants, including Russian and Belarusian nationals, via Russia and Belarus to the EU using existing smuggling infrastructure has continued.[28]

Reports by Member States indicate that together with EU suspects, Ukrainian smugglers remain involved in migrant smuggling activities to the EU and in the facilitation of secondary movements within the EU.[29] Some of the cases concern facilitation of non-Ukrainian third country nationals aiming to reach the EU via Ukraine or Western Balkan region.[30]

Ukrainian documents, fraudulently used for criminal activities

Member States have already voiced concerns regarding an increased use of Ukrainian fraudulent documents and cases of non-Ukrainian nationals using such documents have been reported. Ukrainian authorities have reported a large amount of Ukrainian documents, fraudulent or stolen, and have highlighted the risks of their misuse.[31] Criminal elements involved in migrant smuggling used Ukrainian documents to facilitate other non-EU nationalities into EU Member States.[32]

The online advertisement of fraudulent documents has shown some connections to the ongoing conflict in Ukraine. Telegram groups originally focused on migrant smuggling from Belarus through Poland were found to host advertisements for smuggling via Ukraine and for fraudulent Ukrainian documents.[33]

- A Russian language Telegram channel was reported for hosting advertisements for passports, IDs and drivers' licenses from various EU Member States, as well as Ukrainian and Russian documents (passports, driving licenses and other official documents). Both genuine and fraudulent documents were advertised on the channel; moreover, blank documents from Ukraine with real stamps from official notaries' offices in Ukraine, allegedly issued between 2014 and 2019, were also advertised.[34]
- An Arabic language Telegram channel was reported for hosting advertisements for forged and stolen travel documents, including Ukrainian passports and ID cards.[35]

In addition, numerous individuals were apprehended attempting to illegally cross the border from Ukraine to the EU using forged documents from other countries that benefit from visa exemption with the EU.[36]

Threat assessment and way forward

The risks of smuggling of Ukrainian nationals is likely to remain low due to their protected status in the EU. However, given the smuggling infrastructure in the region, non-Ukrainian nationals (not legally residing in

[28] Information contributed to Europol by EU MS
[29] Europol Information
[30] Europol information, Information contributed to Europol by EU MS
[31] Europol information, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[32] Europol information; Information contributed to Europol by Operational Partner
[33] JLT migrant smuggling and THB meeting, 11 May 2022
[34] Information contributed to Europol by EU MS
[35] Information contributed to Europol by EU MS
[36] Information contributed to Europol by EU MS

Ukraine) may resort to smuggling services to enter the EU from Ukraine. Ukrainian males may similarly seek facilitation from criminals operating in the region.

Ukrainian documents, genuine or fraudulent, may be used by criminal networks involved in smuggling non-EU nationals, including Russian and Belarusian nationals, to the EU, as well as in other crimes involving the movement of people and illicit commodities.[37]

Along with the use of fraudulent documents to facilitate irregular migrants' entry into the EU, criminals may also revert to organising marriages of convenience or fake adoptions in order to obtain long-term legal stay in the EU.[38]

Given the strong connection between migrant smuggling and digital platforms used by smugglers to enable their activities, the latter may also spread online disinformation to fuel anxiety regarding the development of the crisis in Ukraine and thus attract more potential clients.[39]

In the longer term, increasing food and energy prices and diminished food security caused by the disruption of global supply chains in the Black Sea, sanctions on Russian exports and availability of products worldwide (especially grain, fertilisers, gas and oil) may aggravate existing push factors for migration into the EU. This is likely to apply in particular in the main regions of origin of global migratory flows towards the EU, such as Central Asia, Middle East and North Africa, the Sub-Saharan region and the Horn of Africa.[40]

Trafficking in human beings (THB)

The trafficking in human beings targeting Ukrainian refugees remains a key anticipated risk. However, the number of confirmed cases so far has remained limited.

The trafficking in human beings targeting Ukrainian victims has been has been highlighted as a key risk associated with the Russian war of aggression against Ukraine and the large refugee flows towards the EU prompted by this armed conflict. Sexual and labour exploitation, as well as child trafficking are the main areas of concern in relation to refugees from Ukraine.

From the beginning of the crisis, Europol received information about suspected THB activities targeting Ukrainian refugees, the majority of which were suspicions of sexual exploitation of Ukrainian women, but also on potential THB for labour exploitation or targeting minors for the purpose of illegal adoption schemes[41]. Potential THB activities continued to be reported in countries neighbouring Ukraine, but also in other countries in Europe that may be targeted as destinations by Ukrainian refugees.[42]

However, as of 1 June 2022, only three cases concerning THB for sexual exploitation targeting Ukrainian female refugees have been confirmed. The cases concerned a Ukrainian suspect arrested for attempting to exploit Ukrainian underage victims with whom he had travelled to an EU Member State[43], and Ukrainian women forced into prostitution[44] in European countries.

[37] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[38] Frontex, Implications of the war in Ukraine on cross-border criminal activities - Threat Assessment, 1 June 2022, Limite
[39] Frontex, Implications of the war in Ukraine on cross-border criminal activities - Threat Assessment, 1 June 2022, Limite
[40] Frontex, 04.05.2022, Food Security and Migration: impact of the war in Ukraine in the EU – Strategic Analysis Report.
[41] Information contributed to Europol by Operational Partner
[42] Europol information, JLT migrant smuggling and THB meeting 11 May 2022; Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[43] Information contributed to Europol by EU MS
[44] Information contributed to Europol by EU MS and Operational Partner

In addition to cases where countries have confirmed THB activities, information shared with Europol also referred to indications or suspicions that criminal elements are actively targeting Ukrainian victims; these cases are under investigation and monitoring.

Advertisements on websites and social media platforms, posted by dating and escort agencies, either offering sexual encounters with Ukrainian women or offering facilitated transport to Ukrainian women, have emerged online and point to the potential exploitation of Ukrainian women in the EU[45].

Europol has actively supported an Action Day taking place at the end of May aimed at identifying THB in the online environment with a particular focus on refugees from Ukraine that might be targeted for exploitation (sexual, labour or illegal adoption schemes). The Action Day was organised under the EMPACT umbrella, led by the Netherlands, and was joined by 14 EU and non-EU countries. Suspicious advertisements targeting Ukrainian citizens were identified, together with a variety of platforms that may be used to enable exploitation of Ukrainian victims, as well as other indications such as updates in social media individual profiles to reflect Ukrainian origin, potentially to attract more clients for sexual exploitation.

Additionally, Member States are monitoring or investigating individuals with previous convictions for crimes (including sexual abuse and THB), providing or offering some form of support to Ukrainian refugees. In several cases, these individuals were affiliated with humanitarian activities or organisations. [46]

In one instance, a group of EU suspects were suspected of engaging in labour exploitation of Ukrainian women in the EU.[47] In another case suspicions concerned Russian-speaking criminals offering Ukrainian nationals employment in exploitative conditions.[48]

In addition to the above, investigations are ongoing into potential illegal adoption schemes concerning minors from Ukraine and potential recruitment of Ukrainian minors for THB exploitation.[49]

All cases where THB activities were suspected remain under monitoring by the relevant national authorities in cooperation with Europol.

Threat assessment and way forward

Human traffickers and those seeking to abuse Ukrainian victims can easily disguise themselves among the volunteers offering support to Ukrainian refugees,[50] intercepting potential victims in countries neighbouring Ukraine, offering transport, accommodation and assistance and then grooming them while planning their further exploitation.

Minors, including those arriving to the EU unaccompanied or accompanied by others than their legal guardians, remain highly vulnerable targets for criminal networks aiming to exploit the current crisis and the refugee flows into the EU. Besides sexual exploitation, illegal adoption schemes are one of the highest risks related to potential THB activities targeting minors, including surrogate babies born in Ukraine.

In the future, criminal networks that are already involved in THB and exploitation of victims across the EU may increasingly target Ukrainian refugees, making use of their already established criminal infrastructure. In addition to potential recruitment upon arrival in the EU, criminals may increasingly focus on those vulnerable refugees already relocated to the EU, as they may gradually deplete their financial resources and become more vulnerable to recruitment and exploitation, particularly if host countries and

[45] Europol information
[46] Information contributed to Europol by EU MS
[47] Information contributed to Europol by EU MS
[48] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[49] Information contributed to Europol by EU MS and Operational Partner
[50] Europol information, Information contributed to Europol by EU MS

communities would reduce their support.[51]. In this context, exploitation in the agricultural sector may become a potential threat, as harvest season is starting soon.[52] Trafficking of Ukrainian refugees (single individuals as well as whole families) for social benefit fraud is another potential future trend that should be monitored.

Russian-speaking criminal networks are particularly likely to enhance their recruitment efforts into refugees' communities, strongly enabled by the online environment where they may take advantage of language connections to lure victims into various forms of exploitation.

Sanctions evasion

Checks against Europol's databases revealed that 71 of the 1 083 individuals on EU's sanctions list had been reported previously in relation to serious and organised crime. EU sanctions may push those on the sanctions list to use alternative methods to move funds or invest in countries and businesses where the funds can be more easily concealed.

The scale of sanctions imposed on Russian organisations and individuals by the EU and the wider international community as well as the freezing of all types of assets has been unprecedented. [53] The financial sector in the EU and elsewhere has reportedly been struggling to keep up and implement the comprehensive sanctions regime.[54]

EU efforts to implement sanctions against Russian entities

The Task Force "Freeze and Seize" was set up by the Commission in March 2022 to ensure better coordination of the enforcement of EU sanctions against Russian and Belarusian individuals and companies. One of the aims of the Task Force is to explore the links between assets belonging to persons listed under EU sanctions and criminal activities. In this context, the Task Force requested all Member States to share information on the assets frozen so far in their respective jurisdictions. So far, more than half of the Member States have reported to the Commission the measures taken to freeze assets. **They informed about frozen assets worth EUR 29.5 billion, including assets such as boats, helicopters, bank accounts, real estate and artwork worth almost EUR 6.7 billion. In addition, about EUR 196 billion of transactions have been blocked.**[55]

33 Russian individuals subject to EU sanctions control 1 400 European companies. Real estate, construction, hotels, the financial and energy sector prevail. Germany, United Kingdom, Cyprus[56], the Netherlands[57], Luxembourg and Austria are the European countries that host most of oligarchs' firms. The value of these firms is higher than EUR 408 billion (total assets, book value).[58]

[51] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022 (PL)
[52] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[53] European Council, May 2022, EU restrictive measures against Russia over Ukraine (since 2014), https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/
[54] Financial Times 2022, The flood of Russian sanctions has left banks in need of help, accessible at https://www.ft.com/content/e406742a-24a7-41d3-a823-ff59ec20a743
[55] April 2022, EU Commission, 'Freeze and Seize Task Force': Almost €30 billion of assets of Russian and Belarussian oligarchs and entities frozen by the EU so far, accessible at https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2373, accessed 18/05/2022
[56] Europol information
[57] Europol information
[58] Transcrime, 2022, Crime Tech & Universita cattolica del Sacro Cuore, Inside the matrioska: the firms controlled

Circumvention of sanctions has taken several forms such as spreading money into multiple accounts and doing multiple low volume transactions. These transactions do not generate red flags to be reported as suspicious transactions reports by the Financial Intelligence Units. Another way is to obscure the beneficiaries and legal owners linked to Russia by registering new companies as beneficiaries of previously Russian-related companies under the sanction list. These beneficiaries might be family members, employees of trust or strawmen. The front companies are registered in tax heavens and jurisdictions that did not adopt sanctions against Russia. After the publication of the sanctions' list, entities with links to Russia withdrew from their companies in order to avoid the sanctions.

Authorities in the EU, for example, have referred to recent cases where money has been moved from Russia using methods similar to those known in the past as the Russian Laundromat that entailed laundering illicit funds through a series of transactions that involved several financial institutions.[59] Individuals placed under EU sanctions have also been reportedly attempting to safeguard valuable assets such as yachts by moving them to countries like the United Arab Emirates (UAE), with the use of fraudulent documents.[60]

As a result of the checks performed under the umbrella of **Operation Oscar**[61], **71 suspects** out of the **1 083** currently on the list of sanctions were found to have been reported previously for serious and organised crime in Europol's databases.

In addition, checks performed on companies of interest (either on the EU lists of sanctions or related to sanctioned individuals) confirmed much of the geographic pattern for locations where the companies are registered, as presented above.

EU Member States and third countries that have adopted sanctions measures have established multi-agency enforcement mechanisms to implement the restrictive measures. Such mechanisms include crosschecking data in criminal databases and prioritising the identification of cases concerning sanctions' circumvention. Nonetheless, a series of challenges have been encountered including access to the bank registries on frozen assets and to tax data, carrying out investigations on companies registered in high-risk money laundering jurisdictions or following up on assets that are not directly linked to the sanctioned entities. Moreover, countries face another set of challenges in applying the diversity of measures (legal, financial, transport, immigration sanctions) and asset management, also given the lack of a national regulatory framework for the sanctions in many Member States.

Threat assessment and way forward

Preventive measures implemented by banks on Ukraine-related transactions may be generating conditions for informal financial systems to emerge.[62] The European Commission issued guidance to EU Member States, aimed at addressing the heightened risk that Russian or Belarussian investments pose to security or public order in the EU. In the current circumstances, any investments into critical assets in the EU, directly

by sanctioned 'oligarchs' across European regions and sectors, accessible at https://www.transcrime.it/wp-content/uploads/2022/03/Inside_the_matrioska.pdf, accessed 19/05/2022

[59] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022; The Russian Laundromat was a mechanism allegedly used between 2010 and 2014, largely by or to the benefit of Russian entities, to move billions if illegal funds from Russia into and through bank accounts in eastern Europe, then into banks around the world – Organised Crime and Corruption Reporting Project – The Russian Laundromat Exposed, accessible at https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/

[60] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022

[61] See more details on Operation Oscar in the chapter "A joint response to the Russian war of aggression against Ukraine and its impact on serious and organised crime in the EU"

[62] Financial Crime Digest, p 42

or indirectly related to a person or entity associated with, controlled by or subject to the influence of the Russian or Belarusian government, may be suspicious and may pose a threat for the EU.[63]

Countries that have not imposed sanctions against Russian entities create opportunities for investments. Brokers report on open sources that Russian entities are looking for luxury properties outside of the EU.[64]

Large-scale money laundering criminal networks might be involved in providing services to entities under sanctions to circumvent the restrictions for a fee. They have the infrastructure to organise the export of large amounts of money from Russia through their money-transferred system, management of real estate, legal and financial support services. In addition, Russian entities under sanctions are able to pay the requested fee.

The gold trade has already been used in the past to counter international sanctions. Gold can be easily moved outside digital financial networks, and used for money laundering, as its origins can often be disguised, also with the use of fake documents, false declarations and weak due diligence at gold smuggling hubs.[65] Sanctioned entities could use foreign exchange reserves accessed through illicit gold markets for imports, for funding activities or compensation.[66]

Money laundering

To the moment, limited information has been shared with Europol on investigations into money laundering connected to the war in Ukraine. Nonetheless, the current context does generate vulnerabilities that may be exploited by criminals to launder illicit money.

Prior to the beginning of the war, Ukraine was often highlighted among the countries where illicit profits generated in the EU were laundered by criminals. Moreover, Russian suspects and Russian criminal networks were in the past mentioned as perpetrators of money laundering. [67]

In one example reported recently, Russian-speaking criminal networks are investigated for laundering illicit proceeds through fishing companies. [68]

Other criminal cases suggest that proceeds from cryptocurrency investment fraud schemes are transferred to cryptocurrency wallets set up on dedicated large-scale exchanges. The analysis of these wallets indicates that in certain cases they are held in the name of Ukrainian nationals. [69]

[63] EU Commission, April 2022Guidance to the Member States concerning foreign direct investment from Russia and Belarus in view of the military aggression against Ukraine and the restrictive measures laid down in recent Council Regulations on sanctions https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.CI.2022.151.01.0001.01.ENG&toc=OJ%3AC%3A2022%3A151I%3ATOC

[64] Power Yachts, April 2022, Russian Oligarchs Fleeing Sanctions Are House Hunting In Dubai, accessible at https://power-yachts.com/russian-oligarchs-fleeing-sanctions-are-house-hunting-in-dubai/, Business Insider, March 2022, Wealthy Russian investors are snapping up luxury properties in Dubai amid Western sanctions, a report says, accessible at https://www.businessinsider.com/russians-oligarchs-dubai-properties-sanctions-western-countries-2022-3?international=true&r=US&IR=T; Reuters, March 2022, In Istanbul and Dubai, Russians pile into property to shelter from sanctions, accessible at https://www.reuters.com/world/europe/istanbul-dubai-russians-pile-into-property-shelter-sanctions-2022-03-28/

[65] The Global Initiative against Transnational Organised Crime (GI-TOC), Apr, 2022, accessible at https://globalinitiative.net/analysis/russia-sanctions-illicit-gold-trade/ , accessed on 20/05/2022

[66] The Global Initiative against Transnational Organised Crime (GI-TOC), April 2022, accessible at https://globalinitiative.net/analysis/russia-sanctions-illicit-gold-trade/, accessed on 20/05/2022

[67] Europol information

[68] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022

[69] Europol information, Information contributed to Europol by EU MS

Authorities reported large amounts of cash in possession of Ukrainian refugees fleeing their country. Ukrainian nationals were reported attempting to cross to neighbouring EU countries with cash amounting to EUR 1.5 million in one case.[70] Although such cases may provide indications of potential money laundering attempts, the illicit origin of the assets has not been confirmed with the information contributed to Europol.

Threat assessment and way forward

Russian-speaking criminal networks are likely to intensify their efforts to move criminal finances. In this sense and given the restrictions on formal banking flows, it may be expected that they resort to alternative methods such as the use of money mules or informal money transfer services, as well as cryptocurrency investments or illicit gold trade.

In order to facilitate rapid and effective international payments of externally and internally displaced Ukrainian refugees, policy changes to better accommodate Ukrainian and ensure access by refugees from Ukraine to the EU's financial system have been announced. For example, under the EU law, financial institutions can apply Simplified Customer Due Diligence measures when taking on new customers or before carrying out an occasional transaction in situations.[71] Payment service providers will be able to lower their on-boarding requirements for Ukrainian refugees by accepting even those Ukrainian customers who lack the documentation previously required to open an account.[72] All these measures might mitigate the risk that vulnerable Ukrainian citizens would turn to unofficial and potentially illegal means to inject their money into the financial system.

Fraud schemes (including online fraud schemes)

EU citizens have continued to fall victim to online charity scams building their narratives on the vulnerable situation of Ukrainian refugees. However, fraudsters are also targeting Ukrainian victims, under the guise of offering government support after providing personal and financial details, as well as for social benefit fraud.

Various types of charity frauds attempting to elicit money under the guise of supporting Ukraine or Ukrainian nationals have emerged online, targeting victims across the EU. For this purpose, fake webpages have been established that attempt to solicit money, using URLs that include misleading key words such as *solidarity*, *support*, *save*, and *help* for Ukraine. In addition, citizens might receive fake emails pretending to raise money for support from fraudulent addresses. In some cases, fraudsters impersonate known or popular persons that lead or support the campaigns. Fake web-pages and email impersonation are both techniques that fraudsters managed to quickly adapt to the new circumstances.

Fraudsters are also targeting Ukrainian victims with a view to engage in social benefit fraud using their personal information and identity.[73] Indications have emerged regarding more professional networks targeting Ukrainian citizens with scams via instant messaging services. Criminals promise the victims to receive support payments if they register their personal and financial details on a fake government portal operated by the fraudsters.[74] Another type of fraud targeting Ukrainian refugees concerned criminal

[70] Information contributed to Europol by EU MS
[71] European Banking Authority, EBA April 2022, Statement on financial inclusion in the context of the invasion of Ukraine, accessible at https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2022/1031627/EBA%20statement%20on%20financial%20inclusion%20in%20relation%20to%20Ukraine.pdf
[72] Financial Crime Digest
[73] Information contributed to Europol by EU MS
[74] Information contributed to Europol by Operational Partner

elements luring Ukrainian nationals into paying fees for various services such as accommodation or work opportunities, after which the suspects disappeared.[75]

Threat assessment and way forward

Charity frauds perpetrated in the background of the war in Ukraine are likely to continue, given the significant humanitarian mobilisation in support of Ukrainian refugees in all EU MS, delivering a wide range of potential victims. Due to increased awareness and prevention campaigns, methods used for fraud might become more complex and may include impersonation of Ukrainian nationals, use of fake websites for donations or collection of personal information to be used in scams, by various means.

On a longer term, upon the end of the war, given the prospect of significant funds being directed to Ukraine to support the rebuilding of the country, criminal elements may employ fraudulent methods to gain access to such funds.[76]

Excise fraud

Despite obstacles stemming from the war, tobacco smuggling continued at EU's eastern borders. Same actors might be involved, as the modi operandi are the same as those used by criminal networks in the past to smuggle illegal cigarettes into the EU.

Excise fraud involving the smuggling of illegal tobacco products to the EU has been one of the most prolific criminal activities carried out by criminal networks and suspects from Ukraine and Belarus, both key source countries for illicit white cigarettes distributed in the EU. Moreover, in recent years, criminal networks have been setting up illegal production facilities in distribution markets in Western Europe and Ukrainian nationals were often found to work in these facilities.

Despite obstacles that may be expected to result from the ongoing war with regard to illicit movements of people and commodities from Ukraine to the EU, it appears that cigarettes and tobacco smuggling has continued, with EU countries bordering Ukraine reporting seizures or suspicious activity in the area.[77]

Along with seizures of cigarettes transported in buses, unauthorised drone flights on the border with Ukraine, smuggling illegal tobacco from Ukraine, were detected since the war broke out. This modus operandi has also been used in the past by smugglers operating in the region. [78]

Criminal elements were also under suspicion of planning larger shipments of tobacco products from Ukraine to EU countries.[79]

Threat assessment and way forward

While to the moment there is no confirmation on the actors involved, it is possible that the criminal networks previously involved in cigarette smuggling in the region, particularly Ukrainian and Belarusian, continue their criminal activities.

[75] Information contributed to Europol by EU MS
[76] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[77] Europol information; Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[78] Europol information
[79] Information contributed to Europol by EU MS

While most cases and suspicions concerned cigarettes or tobacco products, other commodities may be targeted by criminal elements for excise fraud, particularly with the suspension of taxes for exports from Ukraine into the EU.[80]

Organised property crime

Motor vehicle crime appears to continue undisrupted. Looting of cultural sites has been reported in Ukraine and may deliver opportunities for criminal networks.

There are indications that motor vehicle crime across Ukrainian borders may have continued despite challenges deriving from the ongoing war. Nonetheless, to the moment, no concrete investigations have been reported to Europol, that may be directly linked to the war in the country.

The large number of vehicles with export license plates reportedly queuing to enter Ukraine from the EU may indicate a potential increase in the export of vehicles from the EU to Ukraine, benefitting from tax exemption. Vehicles stolen in the EU may be concealed among legally exported vehicles.

Other reports referred to boat engines stolen from EU countries detected in trucks with Ukrainian license plates.[81] Stolen vehicles from the EU may be smuggled to Ukraine, some possibly in response to the need for vehicles expressed by Ukrainian combatants. Concerns regarding the movement of stolen cars were raised also in the opposite direction, from Ukraine to the EU.[82]

Refugees arriving from Ukraine with larger amounts of cash or valuable objects have already become targets of criminals involved in property crime in EU Member States.[83]

According to Ukrainian law enforcement, looting and property crime have increased in Ukraine since the war began.[84]

Threat assessment and way forward

Ukrainian citizens fleeing from their country with cash or valuable items, as well as those selling their cars at a low price[85] may generate opportunities for potential property crime activities. From a broader perspective, the rise in prices for raw materials across the EU may provide an incentive for increases in thefts.

The need for vehicles on the battlefield as well as the demand for luxury cars and spare parts for the Russian market may attract criminals into new profit opportunities.

Moreover, if EU prices increase for petrol or raw materials such as metal increase, criminal elements are likely to profit from the opportunity and EU MS may witness a spike in thefts of such commodities.[86]

[80] European Parliament, Press release, May 2022, Suspension of EU import duties on Ukrainian exports set for fast-track approval, accessible at https://www.europarl.europa.eu/news/en/press-room/20220516IPR29639/suspension-of-eu-import-duties-on-ukrainian-exports-set-for-fast-track-approval
[81] Europol information
[82] Europol information
[83] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[84] Europol, meeting with the Heads of Criminal Police from EU Member States and the Ukrainian Liaison Officer to Europol on Coordinated Law Enforcement Approach to Ukraine, 4 April 2022
[85] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[86] Europol, Organised Property Crime EMPACT meeting, 03 June 2022

As Ukraine hosts numerous cultural sites, the threat of criminals exploiting the war to loot and smuggle artefacts and cultural vestiges from the country is to be considered and may become more visible in the long term.

Drugs trafficking

No major shifts in drugs trafficking activities have been reported so far in relation to the war in Ukraine. Nonetheless, a change in the routes used by criminals to smuggle drugs into the EU may be expected, given the geographic position of Ukraine and Russia.

Very limited and disparate information has been contributed to Europol since 24 February 2022 on drugs trafficking. Reports concerned, for example, a vehicle potentially carrying drugs from Ukraine that may have been detected in an EU Member State or drugs concealed in humanitarian shipments allegedly travelling from the EU to Ukraine.[87] Information shared with Europol confirmed cargo loads and trains among the preferred means for moving drugs used by criminals.[88]

Threat assessment and way forward

Threats continue to stem from potential shifts in drugs trafficking routes, such as a rerouting of the heroin trafficked through Russia and Ukraine to the EU via the Northern and the Caucasus route respectively, to the Balkan route.

With the port of Constanta taking over much of the sea trade after the Russian blockade of the port of Odessa in Ukraine, there is a risk that heroin trafficking might increase through the former, as well as through the Varna port in Bulgaria. Odessa was also known in the past as an entry point for acetic anhydride arriving to the EU; therefore, criminal networks smuggling it may be forced to find alternate routes into EU Member States.[89]

Ukraine and Russia were previously known as destination countries for drugs arriving through entry points in north-western Europe. With the trafficking infrastructure in place, drugs like cannabis and cocaine may continue to flow through the EU towards EU's Eastern neighbouring countries, through ports in Western Europe.[90] Furthermore, an increase in prices for drugs in Ukraine may also drive an increase in trafficking of drugs towards the country, including from EU Member States.[91]

Similarly, drugs traffickers may use humanitarian convoys to conceal drugs shipments aiming to reach Ukraine.

[87] Information contributed to Europol by EU MS and Operational Partner
[88] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[89] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[90] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April
[91] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022

Terrorism and foreign fighters

There are limited indications of potential terrorist threats emerging from or in relation to the war in Ukraine. Foreign Fighters, including some affiliated with or exposed to violent extremism, may pose risks for the EU's security upon return, particularly given their experience gained on the battlefield.

Foreign Fighters have joined either sides of the conflict. Many have enlisted in the Ukrainian 'International Legion of Defence of Ukraine', a process that has been intensely encouraged also by official actors through online platforms.[92] According to yet unconfirmed assessments of the Ukrainian government about 20 000 volunteers have joined the International Legion. [93] Foreign Fighters arrive from several countries in the world, including many from Europe.[94]

Compared to the Foreign Fighters fighting in Eastern Ukraine in 2014-2016, either on the Ukrainian or the pro-Russian separatist side, who showed a higher ideological alignment with right-wing or left-wing extremism, experts believe that the present wave of Foreign Fighters is less ideologically and politically motivated.[95] The Foreign Fighters joining the battleground in 2022 mostly include regular citizens and army veterans willing to support the Ukrainian national cause, rather than extremists.

According to open sources, some Foreign Fighters already returned home or resigned from the International Legion. Motives for resigning include unfulfilled ideological expectations, health issues, underestimating the life threat posed by the war and the fighting conditions , lack of combat experience or that of adequate equipment, and distrust in fellow Foreign Fighters.[96]

Up to the moment of writing this report, there is no confirmed information on proscribed terrorist organisations formally taking part in the conflict in Ukraine. However, this does not exclude participation in the battlefield from individuals supporting or adhering to extremist ideologies

Online reactions have emerged from terrorist and violent extremist groups and supporters, both from EU MS and from outside the EU.

Violent extremist and terrorist right-wing groups have been active in online calls for joining the fight in Ukraine or for participating in campaigns to finance right-wing actors on the battleground, such as those associated with the Azov Battalion. Popular channels such as Telegram, VK, Twitter, TikTok, Odysee, Gab (a social networking service known for its far-right user base) and 4chan have been used. Most of the messaging originating from EU-based violent extremist and terrorist right-wing groups was pro-Ukrainian, but in several instances, pro-Russian right-wing activity was also identified online.[97] Videos and images of war crimes being committed by alleged members of the Azov battalion fighting for Ukraine, associated with right-wing ideology, have been circulating on social media, however the authenticity of these images is hard to verify.[98]

[92] Legion of Ukraine, Join the International Legion of Defence Of Ukraine, accessible at https://legionofukraine.com/
[93] Alarabiya News, March 2022, Approximately 20,000 foreign volunteers in Ukraine: FM, accessible at https://english.alarabiya.net/News/world/2022/03/06/Approximately-20-000-foreign-volunteers-in-Ukraine-fighting-against-Russians-FM
[94] Europol information
[95] International Centre for Counter-Terrorism (ICCT), May 2022, Foreign volunteers in Ukraine: security considerations for Europe, accessible at https://icct.nl/publication/foreign-volunteers-in-ukraine-security-considerations-for-europe/
[96] Vice.com, March 2022, Returning Soldiers Reveal the Dark Side of Life in the Ukrainian Foreign Legion, accessible at https://www.vice.com/en/article/y3v4xj/joining-ukrainian-foreign-legion
The Brussels Times, March 2022, Over half of Belgian volunteers have returned from Ukraine, accessible at https://www.brusselstimes.com/212437/over-half-of-belgian-volunteers-have-returned-from-ukraine
Telegraaf.nl, March 2022, Ex-soldier back from Ukraine, accessible at https://www.telegraaf.nl/nieuws/530655495/ex-militair-terug-uit-oekraine-twee-keer-aan-de-dood-ontsnapt
[97] Europol information
[98] Europol information

Over the last three months, online activity linked to the war in Ukraine included posts with photographs or personal details of combatants fighting for either the Ukrainian or the Russian side; in some cases, the personal details allegedly belonged to individuals affiliated with right-wing extremism. Several posts originated from right-wing channels and aimed at revealing the identity or whereabouts of enemies[99] or at glorifying allied Foreign Fighters.[100]

Online activities, including those originating from right-wing channels, continued to include calls for recruitment[101], financing campaigns, sale of right-wing paraphernalia, posts presenting travel routes for those interested in joining the fight in Ukraine, or advertising combat successes.[102]

Content identified by experts monitoring online activity identified indications that some members of right-wing groups are active on the battleground, either on the Ukrainian side or on the pro-Russian side.[103]

Threat assessment and way forward

The terrorism element associated with the war in Ukraine is limited. No proscribed terrorist groups are known to formally participate in the war in Ukraine. However, this does not exclude risks of extremists taking part in the fight, returning to the EU and ultimately perpetrating or attempting to orchestrate attacks in Member States. Moreover, the war in Ukraine may be exploited by terrorist and extremist groups to spread their message and ideology, to instigate or attract followers.

Returning Foreign Fighters may have an indirect impact on the terrorist threat posed to the EU as they may become veteran heroes within the EU violent extremist scenes, inspiring or attracting more followers. Furthermore, their combat experience, skills, contacts and networks, access to and knowledge of weapons could make them attractive for violent extremist or terrorist groups active on EU soil as trainers, recruiters or suppliers (of weaponry, for example). Fighters and volunteers may become radicalised on the battleground as they may be exposed to highly ideologically motivated environments and groups.[104]

Returning Foreign Fighters travelling back to EU Member States may engage in violence. However, disillusion may also result in disengagement from their initial motivations.

Foreign Fighters may commit war crimes or be guilty of crimes according to EU Member States' national legislation (for instance, treason) on the territory of Ukraine.

Propaganda activities of EU violent extremist and terrorist right-wing groups will also likely continue, especially aiming at organising travel or financing the presence of violent actors associated with these groups in Ukraine.

Disinformation

Disinformation related to the war in Ukraine has continued. The use of popular online platforms increases the exposure of a wider EU audience and may fuel violent extremist narratives.

[99] Europol information
[100] Europol information
[101] Europol information
[102] Europol information
[103] Europol information
[104] International Centre for Counter-Terrorism (ICCT), May 2022, Foreign volunteers in Ukraine: security considerations for Europe, accessible at https://icct.nl/publication/foreign-volunteers-in-ukraine-security-considerations-for-europe/

Disinformation continues to circulate widely amidst the Russian war of aggression against Ukraine, predominantly disseminated by pro-Russian actors, using a variety of channels and aiming at downplaying the role of Russia as an aggressor. Media outlets keep playing an important role preliminarily addressing Russian-speaking population with distorted war narratives. Social media platforms and instant messaging are a key channel to spread misleading information and propaganda messages.

Disinformation and fake news are heavily used to manipulate the public opinion. Investigations have discovered so-called "troll factories" where groups supporting the Kremlin are believed to employ staff to amplify the reach of posts in order to attract more recruits and mobilise supporters. Traces of these operations were observed on several platforms, including Telegram, Facebook and Twitter.[105] Moreover, disinformation is also used to lure users into fraudulent donations to support population affected by the war. For example, fake livestreams on TikTok have drawn a significant amount of views. In many cases, users post images of an unrelated conflict or dub the sound of explosions and shootings in the background to request donations on their channels.[106]

Deep fakes continued to be used. Recently, mayors of European capitals Berlin, Vienna and Madrid were deceived into carrying online video calls with a 'digitally enhanced' imposter posing as the mayor of Kiev.[107] In addition to the threat resulting from attempts to discredit and undermine the trust in EU authorities and the relations with Ukraine, this form of deep fake may also provide opportunities for accessing sensitive information.

The wave of disinformation may also fuel violent extremist and terrorist narratives in the online environment, therefore indirectly enhancing capabilities for recruitment and financing, and increasing individuals' vulnerability for radicalisation. The lines between disinformation and terrorist and violent extremist propaganda are often blurred, partly due to the lack of capabilities to determine whether certain pieces of information are fake or not.[108]

Threat assessment and way forward

Disinformation actions aiming at weakening the trust of people in national governments and EU institutions in tackling the impact of the crisis in Ukraine are expected to continue. The risk of extremists using disinformation as an instrument to incite violence and potentially to enforce their capabilities to recruit new followers or finance their activities will remain of concern in the near future.

[105] UK Government, 1 May 2022, UK exposes sick Russian troll factory plaguing social media with Kremlin propaganda, accessible at https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda
[106] BBC, 25 April 2022, Ukraine war: false TikTok videos draw millions of views, accessible at https://www.bbc.com/news/60867414
[107] Washington Post, June 2022, European mayors duped into calls with fake Kyiv mayor, accessible at https://www.washingtonpost.com/politics/european-mayors-duped-into-calls-with-fake-kyiv-mayor/2022/06/25/76365a90-f499-11ec-ac16-8fbf7194cd78_story.html, Twitter channel of the Governing Mayor of Berlin, accessible at https://twitter.com/RegBerlin/status/1540375541567602688 ; Official website of Kyiv City Council, June 2022, accessible at https://kyivcity.gov.ua/news/vitaliy_klichko_vorog_vede_viynu_po_vsikh_frontakh__zokrema_i_z_dezinformatsi_z_diskreditatsi_ukranskikh_politikiv/
[108] Europol's specialists in the Internet Referral Unit (IRU) have been monitoring the online activity of EU-based violent extremists, terrorists and their supporters, in relation to the invasion of Ukraine. An accurate analysis of the veracity of information, its origin and targets of the narratives seen in disinformation, as well as its geographical dimension is often challenging. This type of analysis is performed by the European External Action Service (EEAS) that produces a recurrent Disinformation Digest in the context of the EU Integrated Political Crisis Response (IPCR).

War crimes

There are strong indications of military forces committing war crimes in Ukraine. Russian troops in particular appear involved in large-scale violence and human rights abuses against civilians. Serious offences such as murder, rape, torture and illegal detention are widely reported.[109]

According to Ukraine's General Prosecutor's Office, more than 18 000 war crimes have been recorded and 623 suspects are being investigated, including ministers, military and law enforcement personnel, and pro-Kremlin instigators and propagandists (Fig. 1).[110]

Ukrainian law enforcement authorities have issued requests for checks and for the extradition or detainment of Russian suspects, including high-ranking Russian military officers involved in the war in Ukraine, investigated for criminal violations of Ukrainian law.[111]

In addition to the large number of cases opened by Ukraine and based on information available in Europol at the moment of writing this report[112], at least 19 investigations have been initiated in EU and non-EU countries with regard to war crimes committed in Ukraine. Out of the 19, four are structural investigations, allowing for general evidence collection on war crimes (therefore, not conditioned by the existence of one or several identified suspects). Europol has received requests and contributions of war crimes related events and suspects and will continue to provide operational support and expertise to core international crimes investigations under its mandate.

A Joint investigation Team (JIT) has been set up by Eurojust, with participation from Ukraine, Lithuania, Poland, Estonia, Latvia and Slovakia and the Office of the Prosecutor of the International Criminal Court

Fig. 1: Ukraine Prosecutor General's Office - Crimes committed during full-scale invasion of the Russian Federation (Source: https://www.gp.gov.ua/)

[109] New York Times, 2022, Investigators find evidence of war crimes in the Kyiv suburb of Irpin., accessible at https://www.nytimes.com/live/2022/05/03/world/ukraine-russia-war-news#investigators-find-evidence-of-war-crimes-in-the-kyiv-suburb-of-irpin

[110] Ukraine General Prosecutor's Office, 2022, Crimes committed during full-scale invasion of the Russian Federation, accessible at https://www.gp.gov.ua/ (accessed on 21 June 2022)

[111] Requests sent by Operational Partner to Europol

[112] As of 23 June 2022

(OTP-ICC) in The Hague. The aim of the JIT is to support and facilitate investigations into core international crimes, to enable information exchange and ensure the collection and safeguarding of evidence.[113] While currently not part of the JIT, Europol has engaged with its EU and relevant non-EU law enforcement partners and agreed to organise a centralised data collection on war crimes committed in Ukraine and to coordinate and support related investigations in the EU and beyond.

Threat assessment and way forward

War crimes in Ukraine may be perpetrated by all participants in the conflict, including EU citizens that joined the fight on either side. EU citizens may also become victims of war crimes in Ukraine.

Moreover, perpetrators of war crimes in Ukraine may flee the conflict to hide in the EU. Law enforcement in the EU as well as relevant judicial authorities and EU agencies must therefore prepare and join efforts with all relevant partners to collect, preserve and exploit evidence concerning war crimes perpetrated in Ukraine, to support investigations against suspected perpetrators.

Intellectual property crime

The effects of the war on goods' trade with and between EU MS, Ukraine and Russia may drive an increase in trademark infringements and in smuggling counterfeit or sub-standard goods.

EU sanctions include a ban on the import and export of certain commodities from or to Russia. Private sector companies have also imposed their own forms of sanctions, suspending their operations in the country, in order to reflect their stance against the war. Overall, this resulted a significant decrease of accessibility to many products in Russia.

Russia has announced in a decree on 6 March 2022 several countermeasures against so-called "unfriendly States". The countermeasures concerning Intellectual Property Right (IPR) foresee an explicit reduction of protection measures for trademarks and copyrights for "unfriendly" companies and other entities from these States. Concretely, the Russian government has adopted a decree allowing Russian local entities and individuals to use inventions, utility models and industrial designs held by owners from "unfriendly States" without the consent from the IPR owner. This also prevents brand owners from claiming compensation and ownership in Russia.[114] In addition, Russia might legalise some software piracy to mitigate sanctions.[115]

A number of new trademark applications were reportedly filed in Russia in April-May 2022, with new logos clearly resembling those of private companies that suspended their activities in Russia. In a recent decision, a Russian court dismissed a trademark infringement claim from a UK-based company and authorised the use of a version of the trademark Peppa Pig (a popular cartoon series), without consent to the trademark owner.[116] As another example, three days after McDonalds announced its withdrawal from the Russian

[113] Eurojust, March 2022, Eurojust supports joint investigation team into alleged core international crimes in Ukraine, accessible at https://www.eurojust.europa.eu/news/eurojust-supports-joint-investigation-team-alleged-core-international-crimes-ukraine; Eurojust, April 2022, ICC participates in joint investigation team supported by Eurojust on alleged core international crimes in Ukraine, accessible at https://www.eurojust.europa.eu/news/icc-participates-joint-investigation-team-supported-eurojust-alleged-core-international-crimes; Eurojust, Press release, 31 May 2022, Estonia, Latvia and Slovakia become members of joint investigation team on alleged core international crimes in Ukraine, accessible at https://www.eurojust.europa.eu/news/estonia-latvia-and-slovakia-become-members-joint-investigation-team-alleged-core-international

[114] Russian Presidential Decree No 299, 6 March 2022, accessible at http://publication.pravo.gov.ru/Document/View/0001202203070005?index=0&rangeSize=1

[115] Torrent Freak, *Russia Will Probably Legalize Some Software Piracy to Mitigate Sanctions*, published on 07/03/2022, accessed at: https://torrentfreak.com/russia-will-probably-legalize-some-software-piracy-to-mitigate-sanctions-220307/

[116] JDSUPRA, *Peppa Pig: Intellectual Property Infringement as a Form of Retaliatory Sanction*, punished on 25/04/2022, accessed at: https://www.jdsupra.com/legalnews/peppa-pig-intellectual-property-1376654/

market, a Russian fast-food outlet known as 'Uncle Vanya's' filed a new trademark logo replicating McDonald's logo, with only minor variations.[117]

Threat assessment and way forward

Trademark infringements of companies that have taken the decision to suspend their activities pose a threat in the short and medium term.

It is likely that the lack of original products of luxury brands could lead local industries to meet demand by creating imitations and look-alikes products. This could lead to the development of an internal counterfeiting market in Russia, which will possibly increase brand counterfeiting produced in Russia. Another associated risk concerns illicit imports of branded products and of counterfeit products towards Russia considering that the country has been a major importer of EU-based producers such as those from the Italian market.

The agri-food industry might also be affected with infringements of the declaration of origin in Russia. The disruption of food supply chains remains a threat especially for goods for which Ukraine was a significant supplier. This would create opportunities for criminals to penetrate the legal supply chains with unauthorized or unapproved agri-food products.

Other threats

Illicit commodity smuggling

The Russian war of aggression against Ukraine has already produced severe economic consequences, particularly as it had just recovered from the economic impact of the COVID-19 pandemic.[118] Many countries across the world are affected by food insecurity, limited access to energy and raw materials due to trade disruptions, increases in prices and high inflation, among others. EU sanctions are likely to affect commercial routes for commodities, which will most likely have an impact on the routes previously used for smuggling illicit commodities in the EU, particularly on EU's Eastern borders.

With military operations hampering air and maritime trade routes to and from Ukraine, criminals that may have used them previously to smuggle illicit commodities may resort to alternatives such as trains, or may shift to other ports in the Black Sea, as the ones on the Romanian and Bulgarian shores, where large drugs shipments were seized in the past years.[119]

Increased controls on cargo routes may similarly produce changes in the modi operandi used by criminals to smuggle illicit commodities (which might include drugs, firearms, tobacco, stolen, counterfeit or sub-standard goods). [120] For example, criminals may use humanitarian convoys to facilitate the movement of illicit goods to and from Ukraine.

[117] William Fry, *Russia Issues Decree Providing For 0% Compensation for the Unauthorised Use of Certain IP Rights Emanating From "Unfriendly Countries"*, published on 29/04/2022, accessible at https://www.williamfry.com/newsandinsights/publications-article/2022/04/29/russia-issues-decree-providing-for-0-compensation-for-the-unauthorised-use-of-certain-ip-rights-emanating-from-unfriendly-countries

[118] European Commission, Spring 2022 Economic Forecast: Russian invasion tests EU economic resilience, 16 May 2022, accessible at https://ec.europa.eu/info/business-economy-euro/economic-performance-and-forecasts/economic-forecasts/spring-2022-economic-forecast_en

[119] Europol, meeting with the Heads of Criminal Police from EU Member States and the Ukrainian Liaison Officer to Europol on Coordinated Law Enforcement Approach to Ukraine, 4 April 2022; Frontex, Implications of the war in Ukraine on cross-border criminal activities - Threat Assessment, 1 June 2022, Limite

[120] Europol, Meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 7 April

Physical attacks against EU and non-EU targets

Physical attacks on targets from or in countries perceived as enemies by Russian supporters, may pose public safety threats and may be linked to criminals supplying weaponry and explosives to attackers. According to Ukrainian press, grenade launchers were allegedly used against the building of the Moldavian State Security Committee in Tiraspol. [121]

Fugitives relocating to the EU

Europol Guest Officers deployed in the region neighbouring Ukraine supported authorities in two EU Member States in the arrest of two contract killers on the run. The suspects had entered the EU from Ukraine where they had been hiding until the conflict forced them to relocate. One of the fugitives was on the EU Most Wanted list. [122]

Fugitives and other criminals in hiding in the conflict zones may be forced to attempt relocating to EU MS. In addition to the need for law enforcement to monitor such movements, a displacement of fugitives may bring with it more criminality to the EU.

Hate crimes

Hate crimes perpetrated either against Russian nationals or pro-Russian individuals in the EU, but also against Ukrainian and pro-Ukrainian nationals in EU Member States, may be observed in the near future and may affect EU communities' security. Some countries have reported[123] increases in hate crimes manifested through vandalism but also in online conflicts.

Attempts to infiltrate EU agencies and authorities

According to the Dutch General Intelligence and Security Services (the AIVD), a deep-cover Russian intelligence officer attempted to infiltrate the International Criminal Court (ICC) as an intern. A successful infiltration may have produced serious consequences, given the increasingly key role played by the ICC in investigating war crimes in Ukraine and the risks of exposing sensitive information on the proceedings.[124]

[121] Europol information; Liveuamap, April 2022, accessible at https://liveuamap.com/en/2022/25-april-explosions-reported-in-tiraspol-transnistria-near; https://www.jpost.com/breaking-news/article-705070
[122] Europol information, Information contributed to Europol by EU MS
[123] Europol, Second meeting on Mobilisation of the EMPACT community to address and counter serious and organised crime threats linked to the war in Ukraine, 9 June 2022
[124] General Intelligence and Security Services (AIVD), AIVD disrupts activities of Russian intelligence officer towards the International Criminal Court, June 2022, accessible at https://www.aivd.nl/actueel/nieuws/2022/06/16/aivd-verstoort-activiteiten-russische-inlichtingenofficier-richting-internationaal-strafhof

A joint response to the Russian war of aggression against Ukraine and its impact on serious and organised crime and terrorism in the EU

Europol has activated its resources to provide the optimal form of support to EU MS as well as to partner countries directly affected. Europol staff and Guest Officers have been deployed in Ukraine's neighbouring countries (Lithuania, Poland, Hungary, Romania, Slovakia and Moldova) to support the investigations of the countries and perform secondary security checks. Europol continues to work closely with Ukrainian partner authorities. A dedicated liaison officer from the Ukrainian National Police remains embedded at Europol headquarters in The Hague, in order to facilitate communication and support.

Europol is supporting as well the implementation of EU sanctions against Russian individuals by monitoring potential sanction evasions, harnessing its partnerships with the private sector, and particularly the financial services industry through the Europol Financial Intelligence Public Private Partnership (EFIPPP) community. The current EFIPPP efforts include establishment of an EFIPPP Intelligence Taskforce Russia-Ukraine, collecting and sharing Open Source Intelligence and a new Work Stream dedicated to the Circumvention of Sanctions. Furthermore, Europol launched Operation Oscar to crosscheck EU sanctions lists against available operational data, identify links to organised crime and money laundering, produce criminal and financial operational analysis reports, support tracing and seizure of criminal assets and identify beneficial ownership by engaging with private parties. So far, 36 countries have joined the operation.

Through the European Union Law Enforcement Emergency Response Protocol (EU LE ERP) set up to support the collective law enforcement response to large-scale cyber-attacks and cyber crises, Europol's European Cybercrime Centre (EC3) is a part of the constant exchange of intelligence with a variety of partners, including CERT-EU, ENISA, EEAS and many others on the European and national level. Recently EC3 has been in contact with Finish and Swedish authorities in anticipation of potential cyber threats in reaction to their application for NATO membership. Over 30 malware variants being used in cyber-attacks linked to the conflict have been included in the Europol Malware Analysis Solution (EMAS) in order to support Member States investigations. EC3 also carried-out a preliminary analysis based on a list of specific Russian cryptocurrency exchangers provided by the Ukrainian authorities. On this very limited list, no evidence of large sums being transferred by Russians was identified. Given the limitations of this sample and the decentralisation nature of the block chain technology, this does not mean that evasion of sanctions using cryptocurrency is being ruled out.

The Cyber Intelligence Team constantly monitors open sources and disseminates a weekly update on recent activities related to the Russia's invasion of Ukraine to inform Europol's management and Europol's partners on the most relevant cyber developments found in OSINT sources. Additionally, EC3 is informing the general public through awareness campaigns on the criminal exploitation of crisis for personal gain through the use of bogus websites that scam victims into providing their personal or financial information and into donating to fake charities.

Together with EU MS and Ukraine, Europol is also participating in a THB Task Force aimed at tackling the threats emerging from criminal networks that may recruit and exploit vulnerable refugees arriving to the EU.

Online monitoring carried out in Europol also aims at detecting signs of THB activity and material potentially connected to war crimes. Europol has increased its monitoring activities of extremist right wing groups and individuals in the context of the war in Ukraine in order to collect relevant material and information from open source and online media outlets, including information regarding potential war crimes committed in Ukraine. In June 2022, Europol's Analysis Project dedicated to Core International Crimes proposed the establishment of a dedicated OSINT taskforce comprised of experts from different countries, in order to provide targeted support to ongoing investigations into war crimes committed in Ukraine. The Taskforce

aims at supporting OSINT requests from the International Criminal Court (CIC), Ukraine and other countries with active war crimes investigations related to Ukraine.

EMPACT plays a crucial role in the fight against the new threats brought by the war in Ukraine, particularly in the crime areas assessed jointly as immediate or emerging threats. In response to such threats and also to strengthen EU's monitoring and early detection capabilities, EU law enforcement stakeholders, including EU Members States, Third countries and relevant agencies, have initiated efforts towards adapting the EPMPACT framework to the current and potential future challenges. For this purpose, the EMPACT community has mobilised and two meetings were organised on 7 April and 9 June 2022 in Europol, to share information and design the EMPACT response to the crisis and emerging threats. New operational actions have been initiated focusing on High Risk Russian-speaking criminal networks, on New Psychoactive Substances (NPS) and synthetic drugs trafficked on the Eastern borders of the EU, and on criminal finances, money laundering and asset recovery to accommodate the prioritisation of the support provided with regard to implementation of EU sanctions. Additional amendments have been proposed to the existing operational actions agreed in 2021 on THB related to victims from the refugees' flows arriving from Ukraine, including unaccompanied minors, and on migrant smuggling, focusing on document fraud.

Europol will continue to monitor and prioritise the potential developments emerging from the Russian war of aggression against Ukraine and will act as a pivotal element in the European law enforcement cooperation ecosystem, by supporting EU MS and its partners through strategic analysis services, information sharing, crosschecks in databases, establishing links between investigations and sharing expertise and resources.