G7 INTERIOR AND SECURITY MINISTERS' STATEMENT

ELTVILLE, 18 NOVEMBER 2022

OPENING

1. We, the Interior and Security Ministers of the G7, together with the EU Commissioner for Home Affairs, met from 16 to 18 November 2022 at Kloster Eberbach in Wiesbaden, chaired by Nancy Faeser, Federal Minister of the Interior and Community of the Federal Republic of Germany. We discussed the complex challenges that our countries are facing in view of the geopolitical shifts and digitalisation of the economic environment, with a special focus on those created by Russia's unjustified and unprovoked full-scale invasion of Ukraine in February.

2. We build on the final declarations of the previous G7 Interior and Security Ministerial Meetings in 2017, 2018, 2019 and 2021, in which we set our common agenda to address the current challenges based on our shared values.

A. UKRAINE

I. CONTINUED SOLIDARITY WITH AND SUPPORT FOR UKRAINE

3. We, the Interior and Security Ministers and the European Commissioner for Home Affairs, continue to condemn, in the strongest possible terms, Russia's unprovoked war of aggression against Ukraine. Recalling our Joint Declaration from 24 March 2022 and the Statement of the G7 Leaders from 28 June 2022 on the consequences of the war in Ukraine, we remain steadfast in supporting Ukraine and its people.

4. The enormous humanitarian catastrophe resulting from Russia's war of aggression calls for continued joint action of the G7. We have already provided various assistance within Ukraine, in the region and in our home countries for refugees and those forcibly displaced by the war. We will continue to tackle the humanitarian task with joint efforts and call on our partners for continued support. Protecting refugees and those forcibly displaced by the war and especially those most at risk, including women, children and elderly people, remains the highest

priority for us. In addition to our steadfast support for Ukraine, we emphasise our commitment to help the countries in the region as well to support them in responding to the humanitarian crisis resulting from the mass influx of displaced persons from Ukraine and the impact of the conflict on their internal security. The Russian invasion has also produced a global food shortage causing suffering to vulnerable people around the world.

5. We condemn in the strongest possible terms the continuing attacks by Russia against civilian infrastructure and cities across Ukraine. We are deeply concerned about and will follow up on reports of children disappeared in areas under Russian occupation. We reaffirm our commitment to conduct and support investigations of war crimes, conflict-related sexual violence and potential crimes against humanity and genocide. We reiterate that those committing or responsible for such grave crimes need to be held accountable. Important first steps, both nationally and internationally, have been taken, including witness identification by national law enforcement authorities and forensic support as well as coordination initiatives through EU agencies such as Eurojust and Europol and investigations by both national authorities and the Prosecutor of the International Criminal Court.

6. On a daily basis, the world is confronted with new evidence of horrific and despicable crimes committed by Russia and its proxies in the territory of Ukraine. In view of this deteriorating situation and with the aim of bringing those responsible for such international crimes to justice, the G7 Justice Ministers will meet under the German Presidency on 28 and 29 November to discuss measures to improve coordination in cross-border investigations of these international crimes.

7. We confirm our continued effort to support Ukrainian law enforcement authorities through capacity-building measures, training, and provision of urgently needed equipment. Appropriate support will also be provided to the most-affected neighbouring countries of Ukraine to improve the capacity of their response.

8. We will also continue to work closely together to ensure effective implementation of sanctions against Russia and to combat their circumvention by reinforcing our efforts to trace assets of sanctioned persons, by ensuring the investigation of sanctions violations and by working with other countries to block efforts at sanctions evasion. We encourage other countries to take up this critical international effort as well. With regard to G7 activities in the field of implementing sanctions, we will closely observe steps to explore possibilities whether seized assets could be used for the reconstruction of Ukraine consistent with our national laws.

9. We join our Leaders in committing to help Ukraine to rebuild its future.

II. THREATS TO OUR SECURITY

10. Russia's war of aggression against Ukraine has had a significant impact on the internal security of G7 countries. We commit to further strengthening our internal security in direct response.

11. Previous armed conflicts have shown that criminal networks make use of these situations to their advantage. Therefore, we remain deeply concerned that criminal networks could also exploit the movement of refugees, forcibly displaced persons and the war situation in Ukraine. We already recognise serious risks, such as trafficking in human beings and the smuggling of migrants.

12. We are addressing the threat of firearms trafficking by working closely with authorities in Ukraine towards a strict arms control regime and comprehensive registration regime to the extent possible to impede the illicit trading of firearms, explosives and ammunition from the conflict areas. Furthermore, we are closely monitoring the risk of weapons introduced by Russia being diverted. In this respect, the G7 also welcomes the release of the U.S. Plan to Counter Illicit Diversion of Certain Advanced Conventional Weapons in Eastern Europe and supports the work by the EU on a European Action Plan to combat trafficking in small arms and light weapons (SALW) in the context of Russia's war of aggression against Ukraine.

13. We see that some nationals and residents from G7 countries and other countries are travelling to Ukraine on their own to participate in the armed conflict. Amongst these volunteers, most are motivated by support for Ukraine, but there are a small number whose battlefield experience could pose a heightened threat upon their return. We commit to closely monitoring the possible risks these returning volunteers could pose to our internal security.

14. We will continue to counter these phenomena across the whole spectrum: preventing, investigating and pursuing acts, and we call on our international partners to do likewise and to cooperate closely with us.

15. Close cooperation based on trust with all relevant international actors is essential both now and as we support Ukraine in its efforts to defend its borders, protect its people, and ultimately rebuild its country. This includes key partner countries, international organisations, civil society, and the private sector. In the field

of security authorities, cooperation with INTERPOL, Europol and the judicial sector is crucial.

B. FIGHT AGAINST HYBRID THREATS, FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

16. We stand up for democratic values such as freedom of expression, free formation of opinion and the sovereignty of the people. Foreign autocratic actors willingly abuse this open approach to society to serve their own goals.

17. Hybrid threats come from state and nonstate actors who use and blur covert and overt means to spread insecurity, to undermine trust in public institutions, and to sow division within a country and among international community partners and allies. These hybrid threats to our critical infrastructure in addition to information manipulation have increased significantly since the start of Russia's war of aggression against Ukraine. We condemn all foreign malign activities that are directed at undermining our societies and that threaten the integrity of our critical infrastructure.

18. Hybrid threats, including information manipulation and interference, are a growing challenge for democratic societies, governments, and institutions around the world, demanding heightened international collaboration as we look to coordinate united responses from like-minded countries. We therefore welcome the G7 Media Ministers' Communiqué reflecting how media policy contributes to tackling this challenge. Together, we will stand up for our principles and make our democracies more resilient while at the same time pushing back any manipulative attempts to undermine confidence in our democratic institutions. In this context, we will continue to focus and expand our efforts in the G7 Rapid Response Mechanism to counter foreign interference in our democracies including by spreading disinformation.

I. DETECTING AND COUNTERING INFORMATION MANIPULATION NETWORKS

19. We continue to condemn in the strongest possible terms Russian and other information manipulation, including disinformation and other interference by authoritarian governments in our democracies that seek to sow distrust of the democratic order within our countries. While Russia exerts complete control over its own information environment, it takes advantage of the free flow of information in

our democracies to interfere in and attempt to manipulate our citizens' freedom to form their opinions independently.

20. We will increase collaboration to detect malign networks that deliberately disseminate manipulated information in the information sphere. We call on online platforms to enforce their terms of service and thus to address and prevent the spread of disinformation and to take action against inauthentic behaviour, manipulated content and networks of actors with misleading profiles, as well as to continue improving the corresponding mechanisms that enforce these measures. We support online platforms' efforts to make further progress in this area, especially in countries that have less economic relevance for revenues but where these platforms can have a broad negative or manipulative effect on societies. We will work with democratic and like-minded affected states worldwide to advocate for a global response by platforms and the international community to protect our societies from interference.

II. FOSTERING RESILIENCE THROUGH A WHOLE-OF-SOCIETY APPROACH

21. Tackling hybrid threats requires a broad range of responses; one of the key elements is to increase societal resilience. Fostering resilience includes promoting critical thinking skills and media literacy in all age groups as well as building strong networks within society to encourage healthy user practices and habits, and sustaining civic engagement at the national and subnational level. Developing credible public campaigns in a whole-of-society approach will build a broad base of trust. Together, we will amplify the strength and benefits of democracies and the freedoms they guarantee for every citizen, especially in contrast to autocracies.

22. We will establish a comprehensive approach that describes short-, medium- and long-term measures against foreign information manipulation, including disinformation. We are committed to investing in research to learn more about the impacts of foreign information manipulation on democracies and non-democracies alike. Transparency also has a key role to play. We call on online service providers to provide data access for researchers to better understand the scope, scale, and reach of information manipulation and the interventions which can best counter this threat.

23. As we see a rising threat caused by foreign interference at the subnational level, we will intensify our exchange on this matter across different levels of government. The subnational level plays an important role in identifying and countering foreign

interference. Coordination in line with *the whole-of-government* and *whole-of-society* approaches at national, subnational and local level is necessary to identify and counter hybrid threats successfully.

III. STANDING TOGETHER FOR AN INDEPENDENT MEDIA SYSTEM AND AGAINST STATE-CONTROLLED PROPAGANDA CHANNELS

24. Foreign government officials along with state-controlled media, are increasingly manipulating facts and distributing disinformation in our democracies and beyond. These efforts undermine democratic values such as freedom of expression, access to information, the free formation of opinion and freedom of the media. Further, while autocratic states complain of restrictions on their interference in liberal societies, they contradictorily impose much harsher restrictions on independent media outlets and online services in their own countries. This involves routine censorship and threats, imprisonment or even murder of journalists.

25. Besides propagating disinformation and misinformation through their own official channels, autocracies also covertly apply pressure on media outlets established in democratic and other countries, especially media published in languages spoken by diaspora communities. Autocracies deploy coercive methods such as pressuring and intimidating journalists, editors and advertisers to limit discussion of certain topics. These intrusions on our populations' freedom of expression are unacceptable.

26. Considering the destructive character of such foreign interference, we will, with combined efforts, further engage in a meaningful discourse on how to respond to the dissemination and visibility of foreign information manipulation and disinformation while at the same time safeguarding the values we seek to protect with their application.

C. ECONOMIC SECURITY AS AN ELEMENT OF NATIONAL SECURITY

27. Recent developments including Russia's war of aggression against Ukraine underline the importance of protecting critical infrastructure. We recognise with concern the increasing efforts of hostile state actors to obtain expertise and technology through industrial espionage, malign tradecraft and other forms of covert intelligence collection. The alleged sabotage of gas pipelines in the Baltic Sea reveals the need to better protect our critical infrastructure. Therefore, developing stronger overall security awareness while exploiting best practices and building

partnerships at the national and international level, including with the private sector, is crucial to become more resilient.

28. We see a period of continued heightened cyber threat. Collateral effects in G7 countries are already taking place. The number and heterogeneity of the actors involved in the conflict in cyberspace, such as state-controlled groups or so-called hacktivists, lead to complex threat situations to information and communications technology infrastructure, with the potential to escalate.

29. We will deepen our strategic cooperation among the G7 in countering attacks on and better protecting our critical infrastructures by leveraging our collective analytical resources to prevent, detect and counter all forms of malicious activities such as acts of sabotage and espionage against or disruption of our critical infrastructure.

30. Beyond critical infrastructure, we must protect the private sector and research communities from hostile activities conducted by state actors, state-controlled proxies or criminal organisations, including through means such as malign foreign investments, takeovers, malicious cyber activities and criminal outflow of proprietary information. Particularly in these economically challenging times, the state and the private sector must join forces in ensuring that security measures and policies effectively safeguard against hostile activities.

31. A comprehensive picture of the nature and intensity of the threats targeting the business and research communities is essential. It is therefore necessary to identify risks at an early stage and then analyse and mitigate them properly. In this context, we ask the G7 Roma-Lyon Group to regularly discuss the risks and exchange best practices in the field of economic security to strengthen our resilience and ensure our prosperity, stability, freedom and democracy.

32. Additionally, we recommend a continued conversation among G7 countries in all relevant fora on what a whole-of-government approach and effective public-private cooperation might look like in practice and how addressing threats to the economy and research community are best reflected in national security strategies, while encouraging opportunities for economic growth and prosperity and preserving the benefits of an open and collaborative research environment.

D. FIGHT AGAINST ALL FORMS OF VIOLENT EXTREMISM AND TERRORISM

33. We remain dedicated to the fight against all forms of violent extremism and terrorism, both online and offline. We reaffirm the 2021 London Interior and Security Ministers' Commitments in this regard. We join our Leaders with our commitment to intensify our cooperation with all relevant actors to prevent and counter all forms of violent extremism and terrorism. We underscore the important role that the G7 Roma-Lyon Group plays in this context.

34. Violent extremism and terrorism in the sense of different terminologies like extreme right-wing terrorism, far-right extremism and racially, ethnically or other ideologically motivated violent extremism or terrorism, which may incorporate a range of hateful, xenophobic, misogynistic, anti-government, anti-authority and other violent grievances that may lead to mobilisation of violent extremism and terrorism, poses a potentially high threat to G7 countries, with national and possible transnational implications. In particular, the internet and the COVID-19 pandemic have helped facilitate radicalisation to violence; networking beyond national boundaries among individuals, including youth; more lone actors; and the development of loose networks of violent extremists in recent years, all of which provides a challenge for our law enforcement and security agencies.

35. We therefore reaffirm our strong resolve to prevent and counter all forms of violent extremism and terrorism at both the national and international levels and through joint efforts among the G7 countries. In this context, we employ a holistic approach, both offline and online, which combines prevention, detection, response and intervention, and draws on the expertise of all relevant stakeholders. To this end, we pledge to proactively pursue these items on the agenda of forthcoming G7 Interior and Security Ministers' meetings and ask the G7 Roma-Lyon Group to consider a study of respective approaches to prevention and countermeasures in more detail.

36. Strong collaboration and coordination between relevant stakeholders is necessary to properly understand and tackle this evolving threat, including online. We approve collaboration between G7 members, the Global Internet Forum to Counter Terrorism, and the Christchurch Call to Action in developing comprehensive responses. We welcome the first Counterterrorism Law Enforcement Forum, led by Germany's Federal Ministry of the Interior and Community in Berlin in 2022, which focused on domestic violent extremism and brought together more than a hundred

law enforcement officials, prosecutors, and other criminal justice practitioners from almost 40 countries and from key multilateral institutions.

37. The threat posed by ideologically motivated violent extremism and terrorism, including by self-declared Islamist terrorist groups such as Al-Qaeda, ISIS, and their affiliates, is enduring and evolving. The G7 members and their interests and institutions worldwide remain a direct target of various terrorist organisations.

38. Foreign terrorist fighters/returnees from combat zones pose a particular risk. G7 partners are closely monitoring the rising occurrence of foreign fighter flows to and from combat zones, particularly in relation to the risk of radicalisation to violence and other potential threats. We must continue to work together to ensure coordination with respect to these individuals and share information when available.

39. Successful military operations by the worldwide alliance against international terrorist organisations, such as the Global Coalition to Defeat ISIS, have significantly degraded the financial situation of those groups. For example, while ISIS remains a significant threat, the fact that it no longer holds territory has greatly restricted its ability to generate funding. Terrorist actors are therefore attempting to find alternative sources of funding. Clarifying terrorist actors' financing structures is therefore an essential component of the overall strategy to counter international terrorism.

40. Clarifying financial networks, the widespread use of fintech, cryptoassets and any other systems that allow financial resources to be transferred, also anonymously, not only prevents terrorist attacks, but also helps to identify violent extremist activities and to initiate appropriate countermeasures, which may help prevent radicalisation to violence.

E. AFGHANISTAN – SECURITY IMPACTS

41. The situation in Afghanistan continues to pose major challenges for the international community. We remain seriously concerned that Afghanistan may again become a safe haven for terrorists who threaten our countries, partners and interests. We recall in that respect the demands put forward by the international community in Security Council Resolution 2593.

42. Crime phenomena such as drug trafficking have huge impacts on the internal security of the G7 countries. We underscore the need for intensified international cooperation in the fight against drug production and drug trafficking in and from

Afghanistan, with all relevant stakeholders, including affected and neighbouring countries, the UNODC, INTERPOL, Europol and other relevant international organisations. Cooperation with these structures present on the ground is essential to allow the G7 countries to better understand the evolving situation and the evolution of the threats it poses. Our efforts are crucial in tackling the threat and understanding narcotics trafficking from Afghanistan, including its facilitation links with terrorist organisations operating within the country. We will share emerging research, assessments and information in order to enhance our evidence base and work together to improve the global response to the threat.

F. TRANSNATIONAL SERIOUS AND ORGANISED CRIME

43. Transnational serious and organised crime remains a significant threat to both our national and international security, causing damage and threats to society, state institutions and the private sector. Organised crime groups react and adapt flexibly and opportunistically to changing conditions and changing technologies, as they have demonstrated during the COVID-19 pandemic.

44. The main driving force of organised crime is profit-making. Organised criminals deploy a range of sophisticated methods to disguise illicitly acquired wealth. We therefore need to further pursue the “follow-the-money” approach with focus on the financial aspects of illicit activities and strengthen existing organisational structures and workflows on information exchange aimed at detecting, tracking and disrupting illicit finance and combating the concealment of the proceeds of corruption, fraud and other crime. We reaffirm the importance of cooperation across borders to tackle transnational threats and support the work of the FATF, INTERPOL, Europol and other relevant international organisations. In this context, we also underscore the G7 Interior and Security Ministers’ Commitments from 2021, including the Statement against corruption and kleptocracies. We join our Leaders with our commitment to defend the integrity and transparency of democratic systems as set forth in the Statement of the G7 Leaders from 28 June 2022.

45. To further ensure the security of our citizens, we intend to intensify our fight against transnational serious and organised crime, including cybercrime, drug trafficking, trafficking in human beings, child sexual exploitation and abuse, crimes that affect the environment and corruption, in close cooperation with civil society and international actors, such as INTERPOL, Europol and the UNODC. We will continue our cooperation in this field, including in the G7 Roma-Lyon Group, to foster international cooperation to counter transnational serious and organised crime.

46. Organised criminal networks exist, which facilitate dangerous journeys of migrants and asylum seekers, profiting off some of the most vulnerable. We call for firmness in dealing with this ruthless criminality that puts lives in danger and poses a risk to internal security of G7 partners. We need to break the business model of organised crime networks dealing with trafficking and smuggling of human beings to tackle this issue of growing concern.

47. We reiterate our commitments to expand INTERPOL's tools and services in the fight against transnational serious and organised crime, including ensuring that all member countries have access to the tools they need, providing support and information where appropriate, while ensuring that the priorities of G7 members are adequately funded.

48. We recognise that synthetic drugs, including synthetic opioids, methamphetamine, fentanyl and new psychoactive substances, represent a significant developing drug threat. To deter and disrupt global manufacture and trafficking of such drugs, we must increase the costs and risks to criminals engaging in these activities across the entire supply chain. We intend thus to intensify our work to address precursor chemicals, mislabelling, misuse of equipment, illicit finance, and illicit online sales, to engage relevant industries, and to promote drug use prevention, treatment, and recovery.

49. The following crime phenomena are areas of particular concern to the G7:

I. SERIOUS THREATS TO CHILDREN

50. Transnational crime also affects the most vulnerable. Protecting children around the world, both online and offline, from child sexual exploitation and abuse is a global task. We underscore that the protection of our children remains our highest priority. We welcome the recent decision by the UN General Assembly to proclaim 18 November of each year the World Day for the Prevention of and Healing from Child Sexual Exploitation, Abuse and Violence (A/77/L.8). We commit to step up the G7's impact in fighting trafficking in human beings and our efforts to prevent and combat child sexual exploitation and abuse globally, both online and offline.

51. We recognise that the threat to children has been growing and evolving dramatically in recent years, enabled by the criminal misuse of the internet and exacerbated during the COVID-19 pandemic. The internet offers many opportunities for perpetrators to groom, to abuse and to exploit children, to share images and videos depicting child sexual abuse, and to normalise these crimes.

52. We will therefore strive for clear and coherent frameworks that call on the technology industry to keep children safe online. We underscore that building knowledge and capacity of law enforcement officials, prosecutors and judges, especially regarding information and communications technology, and enabling multidisciplinary cooperation at all levels, is a crucial part of the response to trafficking in human beings and child sexual exploitation and abuse.

53. In this context, we recognise the opportunities offered by digital technologies and artificial intelligence, serving as a tool to create a safer online environment for children, to prevent, detect and investigate crimes, and to help identify and assist victims. We underscore the importance of cross-sector cooperation with civil society and the private sector, including the technology and financial sectors, to combat these especially heinous crimes. We support the investment in and development of services that are safe for children by design, protect children's privacy, and innovation to advance the solutions available that allow companies to identify and report child sexual exploitation and abuse. We support technology-neutral innovation and development. We call on industry to endorse and transparently implement the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse considering national legislation.

54. We take note that the increasing misuse of "live streaming" poses a growing threat to the most vulnerable, our children. The modus operandi of "live streaming" lies at the intersection of child sexual exploitation and abuse and trafficking in human beings. "Live streaming" is not only a source of abusive material, in particular where recorded and shared further, but also depicts real-time sexual violence against the victims. The modus operandi has a strong commercial component, and we recognise the importance of engagement with the private sector – technology and financial sectors – to advance the technological solutions and interventions required to combat this crime. Only through international cross sector cooperation are G7 partners able to tackle the challenges linked to the misuse of "live streaming" by tracking financial streams, securing evidence and promoting technological solutions that first and foremost protect the lives of the victims.

55. We commit to take forward the implementation of the G7 Action Plan to combat Child Sexual Exploitation and Abuse announced in September 2021, via the G7 Working Group on Child Sexual Exploitation and Abuse in the framework of the Roma-Lyon Group.

56. We acknowledge the strong role of victims' and survivors' voices to help raise awareness of these horrific crimes and support effective action against them. The G7 will consider and promote the victims' and survivors' perspective whenever measures to end child sexual exploitation and abuse are planned or implemented, aiming to create a safer online world for children, free of sexual violence.

57. As part of the implementation of the Action Plan, and inspired by collective international law enforcement collaboration in South-East Asia, we encourage the G7 Roma-Lyon Group to use targeted projects to combat child sexual exploitation and abuse. A project format allows developing a G7 toolbox combining all G7 capabilities, capacity, knowledge and best practice.

II. CYBERCRIME

58. Organised crime groups make use of modern technological developments, communicate and commit crimes online. We are therefore committed to continuing to advance our cooperation in addressing the fight against serious and organised crime in its online dimension, including by fostering the swift cross-border exchange of information. We urge all countries to develop laws, policies and practices that effectively combat cybercrime, including, if possible, to become party to the 2001 Budapest Convention on Cybercrime and the Second Additional Protocol. We commit to closely work together in the framework of the negotiations of a future UN Cybercrime Convention.

59. One further element is the abuse of the decentralisation and anonymisation of crypto assets, along with the use of anonymisation tools and encryption for criminal purposes. Accordingly, we aim to strengthen law enforcement and judicial cooperation among our nations to locate, preserve and collect electronic records and digital evidence in cases of criminal misuse of technology crypto assets.

60. Cryptocurrency is also the payment method of choice in ransomware attacks. G7 members continue to prioritise the international collaboration necessary to tackling the global ransomware scourge. In November, together with partners from the International Counter Ransomware Initiative, we re-affirmed our joint commitment to building our collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering illicit finance that underpins the ransomware ecosystem, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat. Accordingly, we intend to continue to strengthen

law enforcement cooperation among our nations to preserve vital evidence needed to investigate cybercrimes and identify and bring to justice those who commit them.

III. CRIMES THAT AFFECT THE ENVIRONMENT

61. We reaffirm our commitments made in the September 2021 G7 Interior and Security Ministers' Commitments to counter crimes that affect the environment. We strongly condemn those who profit from crime at the expense of the environment and biodiversity. We commit to take action, together with other relevant Ministers, to contribute to our Members' efforts to combat illicit finance from crimes that affect the environment. We will continue to work together to exchange best practices and recommendations, using the experts' network created under the French Presidency in 2019. We welcome the significant work of key global partners on these issues, including the UNODC, INTERPOL, Europol and other international organisations.