G7 Interior and Security Ministers' Communiqué December 10, 2023 in Mito, Ibaraki



Preamble I.

- 1. We, the G7 Interior and Security Ministers, together with the European Commissioner for Home Affairs and the Secretary General of INTERPOL, met in Mito, Ibaraki on December 8 to 10, 2023. We were also joined by the Interior Minister of Ukraine. We gathered to discuss the global challenges to our safety and security, and renew our commitment to fight against threats to our societies and values.
- 2. We are more united than ever, particularly in the context of an increasingly severe global security situation, to address the current challenges we face, guided by common values and principles, including freedom, democracy, the rule of law, and respect for gender equality and human rights.
- 3. We remain determined to work with our partners to enhance our efforts to counter an array of common challenges and provide our people a safer, more secure, and better future.
- 4. We build on the previous commitments of the G7 Interior and Security Ministers' Meetings since 2017, in which we set our common agenda to address the current and emerging challenges based on our shared values.
- 5. We welcome the ongoing efforts and intensification of cooperation of the G7 Roma-Lyon Group (RLG) to prevent terrorism and violent extremism and counter organized crime under Japan's presidency in 2023.

II. Continued Solidarity with and Support for Ukraine

- 6. Our steadfast commitment to supporting Ukraine's fight for its independence, sovereignty, and territorial integrity will never waver. We once again condemn, in the strongest possible terms, Russia's illegal, unjustifiable, and unprovoked war of aggression against Ukraine. Recalling the G7 Hiroshima Leaders' Communiqué, we reaffirm our unwavering support for Ukraine for as long as it takes to bring a comprehensive, just, and lasting peace.
- 7. We condemn all types of crimes committed in the context of Russia's war. There must be no impunity for war crimes and other atrocities, including Russia's unlawful killings, sexual violence, and torture. In this context, we reiterate our commitment to holding those responsible to account consistent with international law, including by supporting the efforts of the Ukrainian authorities and international bodies such as the International Criminal Court (ICC) and the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA) at Eurojust. We strongly condemn the unlawful deportation and transfer of Ukrainian civilians, including children, to Russia and elsewhere, and will continue to follow the progress of the ICC investigations in this regard with the utmost attention, and call for the immediate and safe return of all children, including those facing heightened risk of trafficking in persons. We reiterate the need for close cooperation between international and national authorities, supported by Europol and Eurojust, to ensure those responsible for international crimes can be held accountable.













- 8. We stand with Ukraine as it seeks to counter the impacts of Russia's war on the Ukrainian people. We thank H.E. Ihor Klymenko, Minister of Internal Affairs of Ukraine, for joining. We discussed a range of subjects including the situation on the ground in Ukraine, and needs of Ukrainian law enforcement authorities in facing a range of threats in both the short and long term. We commit to supporting Ukrainian authorities through capacity-building measures, training, and the provision of urgently needed equipment to take all available steps to protect the people and sovereignty of Ukraine. We recognize Ukraine's ambitious reforms, including on anti-corruption, and welcome the launch of the G7 Justice Ministers' "Anti-Corruption Task Force for Ukraine", and endeavor to coordinate our efforts and seek synergies with the Task Force when providing assistance to Ukraine related to anti-corruption.
- 9. We are determined to deny Russia, Russian entities, and individuals that are complicit in the war the ability to hide and benefit from their assets in our jurisdictions. In coordination with our foreign, finance, and criminal justice counterparts, we will continue to work through the Russian Elites, Proxies, and Oligarchs (REPO) Task Force to enhance the effectiveness of our restrictive measures against Russia, together with the EU Freeze and Seize Task Force and the Task Force KleptoCapture. We recall and reaffirm the G7 Leaders' Statement on February 24, 2023, the G7 Leaders' Statement on Ukraine on May 19, 2023, and the G7 Leaders' Statement on December 6, 2023, along with the G7 Foreign Ministers' Statement on November 8, 2023, that stated, consistent with our respective legal systems, Russia's sovereign assets in our jurisdictions will remain immobilized until Russia pays for the damage it has caused to Ukraine. We reiterate our unwavering resolve to impose and enforce sanctions and other economic measures to further undermine Russia's capacity to wage its illegal, unjustifiable and unprovoked war of aggression. We remain committed to countering any attempts to evade and undermine our sanction measures.

III. All Forms of Terrorism and Violent Extremism

- 10. We reiterate and underline the G7 Leaders' Statement on December 6, 2023 that unequivocally condemned the horrific terror attacks across Israel by Hamas and others that began on October 7, 2023, and call for the immediate release of all remaining hostages without preconditions. The current situation in the Middle East not only poses a threat to global security and has a direct impact on our societies, but also raises humanitarian concerns. We emphasize Israel's right to defend itself and its people against Hamas, in accordance with international law, as it seeks to prevent a recurrence of these traumatic events, which included murder, hostage-taking, sexual violence, and attacks on children. Hamas offers nothing but suffering to the Palestinian people, and it is an obstacle to a better future for them and for the region. We will continue to coordinate our efforts to isolate Hamas and ensure it cannot threaten Israel. We are also deeply concerned with the devastating impact on the Palestinian civilian population in Gaza. Regional actors must cease de-stabilizing activities. We condemn the rise in extremist settler violence committed against Palestinians, which undermines security and stability in the West Bank, and threatens prospects for a lasting peace. Those who have committed crimes must be held to account.
- 11. We express our deep concern with the rise of hateful speech and acts across the world since the beginning of the conflict, and categorically reject antisemitism, anti-Muslim hatred, and any forms of discrimination on the basis of race, religion or belief. It disturbs peace and social cohesion, and above all it threatens Jewish, Muslim, and Arab people. We, the G7 Interior and



Security Ministers and the European Commissioner for Home Affairs, stress our steadfast commitment to act decisively and jointly to protect these people from antisemitism, anti-Muslim hatred, and any forms of discrimination as well as actions incited by violent extremist actors that have been reported across our societies by taking all possible actions, including preventive and educational measures as well as decisive action by our security authorities as appropriate.

- 12. The world continues to suffer from attacks by terrorist and violent extremist groups and lone actors, espousing a range of violent extremist ideologies and inspired by local, regional and global movements of all motivations. In this regard, we reaffirm our strong resolve to prevent and counter all forms of terrorism and violent extremism, both online and offline, at the national and international levels through collective efforts among the G7 members. We reiterate the importance of collective efforts on countering terrorism and violent extremism, and continue to collaborate at the domestic and international levels to ensure our efforts are thorough, appropriate, and effective. We also ensure that our responses respect human rights and fundamental freedoms for all. We continue to increase our capabilities to prevent and counter threats, identify those who pose a risk, and protect populations, in particular at-risk communities, from acts of violence. We continue to emphasize the need for collaborative prevention efforts, using the G7 frameworks such as the RLG to take collective action.
- 13. Terrorists and violent extremists utilize the Internet to disseminate illegal and harmful content, including terrorist and violent extremist content, to finance terrorist and violent extremist activities, recruit individuals to their cause, encourage radicalization to violence, and incite both physical and online attacks. We once again join our leaders in calling on the private sector to step up their efforts to address the dissemination of terrorist and violent extremist content online. We reaffirm our cooperation with the Global Internet Forum to Counter Terrorism (GIFCT) and stress the importance of expanding GIFCT membership to include a broader range of technology companies, as well as helping smaller platforms identify and address terrorist and violent extremist content, in partnership with Tech Against Terrorism. We also reiterate our support for the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online and welcome the achievements made since its adoption in May 2019. We call on the GIFCT and its member companies to renew their commitment to prioritize addressing terrorist and violent extremist content online, in line with the Christchurch commitments, and to do more to address terrorist and violent extremist content, especially the rise in antisemitism and anti-Muslim hatred online since October 7, 2023.
- 14. We emphasize the importance of building and maintaining trust between governments, including law enforcement agencies and the communities they serve, to create a society resilient to threats of terrorism and violent extremism. In this sense, democracy, the rule of law and good governance are essential in fostering effective and non-violent means for addressing political, social and other grievances. We reiterate our strong commitment to work together with all relevant actors, including civil society, to prevent and counter all forms of terrorism and violent extremism, and their financing. This includes countering cross-border movement of known terrorists via information sharing and screening through platforms such as INTERPOL, and ensuring our tools and policies are adapted to respond to the current threat landscape while protecting the most vulnerable.



IV. Ensuring Economic Security

- 15. Recalling the G7 Leaders' Statement on Economic Resilience and Economic Security on May 20, 2023, and the G7 Foreign Ministers' Communiqué on April 18, 2023, along with the commitments from other Ministerial tracks, we also stand strong to do our part in ensuring economic security and countering threats to our democratic values.
- 16. We are faced with both state-led and non-state-led activities that aim to acquire our cuttingedge technologies through exploitation of our open economic systems, economic espionage, evasion of sanctions and export controls, and other forms of covert intelligence collection. Additionally, otherwise-legitimate activities, such as foreign direct investment and provision of Information and Communication Technology (ICT) can be abused by malicious actors to gain access to sensitive assets or data with implications for national security. In accordance with our respective legal frameworks, we will continue to implement export control measures, refine investment screening regimes, and secure supply chains, without unduly limiting trade and investment. We will work with international partners to intensify our collective effort to close gaps in our dual-use technology protection ecosystem and mitigate risks to national security stemming from foreign investments, preventing the exploitation of legitimate economic activity to advance aggression or provocations. We will take action to identify and mitigate risks of disruptions to critical infrastructures underpinning our supply chains.

V. Countering Threats to Peace, Security, and our Democratic Values

- 17. We remain deeply concerned about the humanitarian situation in North Korea, which is driven by North Korea's choice to prioritize its unlawful weapons of mass destruction and ballistic missile programs over the welfare of the people in North Korea. We reaffirm our commitment to ensure effective implementation of sanctions under relevant United Nations Security Council Resolutions and prevent and address sanctions evasion and attempts in cyberspace to steal and launder digital assets. We urge North Korea to respect human rights and resolve the abductions issue immediately.
- 18. We are increasingly concerned by hybrid threats and foreign interference activities, including information manipulation, spread of mis-, mal-, and disinformation, as well as transnational repression, by foreign states or non-state actors acting on their behalf, attempting to sow discord in our democracies across the globe. We join our colleagues and counterparts among the G7 in amplifying the strength and benefits of democracies and the freedoms they guarantee for every citizen, including the freedom of expression. We reaffirm our support for the G7 Rapid Response Mechanism to strengthen the G7 coordination in identifying and responding to foreign threats against democracies. In this regard, we strongly condemn the widespread use of information manipulation and disinformation by Russia and others.
- 19. Recognizing the corrosive impact of these multifaceted threats to societies, we will foster resilience through a whole-of-society approach in protecting our information, technologies, and upholding our democratic values.

VI. Keeping Cyberspace Safe

20. Recalling the G7 Hiroshima Leaders' Communiqué, we reaffirm that governance of the digital economy should continue to be updated in line with our shared democratic values. These



include fairness; accountability; transparency; safety; protection from online harassment, hate and abuse; and respect for privacy, human rights, fundamental freedoms and the protection of personal data. We join our Digital and Tech Ministers in promoting an open, free, global, interoperable, reliable, and secure Internet. At the same time, as the G7 Ministers responsible for security, we are concerned with the ever-increasing dangers that cyberspace can have when misused by actors with malicious intent.

- 21. We remain aware of that the Internet hosts a range of illegal content, including child sexual abuse materials, and harmful content, including content that can facilitate and encourage illegal and violent acts, such as manuals on how to assemble homemade firearms and explosives. We are committed to protecting our citizens from acts of terrorism and violent extremism, child sexual exploitation and abuse, fraud and other crimes that may be accelerated through the use of cyberspace, including by ensuring the appropriate frameworks in place are used. We will also leverage our partnerships with the ICT industry with a view to identifying and responding to such illegal and harmful content from cyberspace as appropriate. We recognize that both governments and the private sector need to work together consistent with domestic legislation and international obligation to ensure an effective approach to illegal and harmful content. We will strengthen our outreach efforts to empower Internet users and civil society on crime prevention related to cyberspace. We will promote public-private partnerships among industry, government, and academia, following best practices of the EU Internet Forum and other relevant international fora and communities.
- 22. We encourage all state and non-state actors to act responsibly in cyberspace. Echoing our Foreign Ministers, we encourage China to uphold its commitments to act responsibly in cyberspace, including refraining from conducting or supporting cyber-enabled intellectual property theft. We will step up our cooperation to counter North Korea's malicious cyber activities. We will collectively take international action to eliminate safe havens from which cybercriminals, such as Russian ransomware actors, can too often act with seeming impunity. We will continue to do our part in promoting the rule of law in cyberspace, countering cybercrime through the utilization of human-rights based international frameworks, and increasing information sharing with partners and strengthening cooperation in investigations in their actions.
- 23. We continue to prioritize the international collaboration that is necessary to confront the global scourge of ransomware, phishing and other cybercrimes, including through fora such as the International Counter Ransomware Initiative. We will strengthen law enforcement and other relevant agencies' cooperation among our nations to identify threats and preserve and obtain vital evidence needed to investigate cybercrimes and bring to justice those who are committing these crimes.
- 24. Emerging technologies in cyberspace, including generative artificial intelligence (Al), offer many opportunities with respect to our work and society. While we must continue to harness the capabilities of these emerging technologies to keep our citizens safe and secure, we must also recognize that these technologies can be misused by criminals, terrorists and violent extremists to further their activities. We also recognize that such technologies can increase the scale of harm and make it more difficult for law enforcement agencies to identify, investigate and prosecute these crimes. To deal with this increased threat, we will continue to share information of the latest modus operandi of illicit activities, leverage our individual and collective











capabilities, including by updating the capacities of our law enforcement agencies, work in partnership with industry to evaluate and minimize the risks of exploitation, promote information integrity, and seek to balance the rights and responsibilities of all stakeholders with a view to protecting the security and privacy of our citizens. We welcome the G7 Leaders' Statement on Hiroshima Al Process on October 30, 2023 as well as the G7 Leaders' Statement on December 6, 2023, and will prioritize the actions called for in the Hiroshima Process International Guiding Principles for Organizations Developing Advanced Al Systems and the Hiroshima Process International Code of Conduct for All Al Actors and Organizations Developing Advanced Al Systems, keeping in mind that our efforts can lead emerging technology development to support the common good worldwide.

25. Online privacy and security safeguards, such as strong encryption, are critical to protecting our citizens online and serve a vital purpose in repressive states to protect journalists, human rights defenders and vulnerable people. However, the rapid implementation of private and secure communication technologies without consideration of public safety and with limited or no consultation with democratic governments poses significant challenges in our ability to protect our citizens. Building on our collaboration to date and recalling previous statements made by the G7, we will work together to maintain tightly controlled lawful access to communications content that is vital to the investigation and prosecution of serious crimes, including terrorism and violent extremism and child sexual exploitation and abuse, and will work in partnership with technology companies to do this to protect the safety of our citizens. In this regard, we call on the private sector to increase their efforts to engage with democratic governments and civil society on secure communication technologies and ensure safety is considered at the design phase, including maintaining tightly controlled lawful access, when developing these technologies. To this end, we encourage the RLG to continue discussing respective approaches and sharing best practices in this field.

VII. Child Sexual Exploitation and Abuse

- 26. We affirm our strong collective commitment to tackle all forms of child sexual exploitation and abuse. Protecting children around the world, both online and offline, remains our top priority. We are concerned with the rise in child sexual exploitation and abuse, and recognize that the Internet, including social media platforms, continues to offer many opportunities for perpetrators to recruit, advertise, lure and groom, "sextort," abuse, and exploit children, share images and videos depicting child sexual exploitation and abuse, including through "live streaming," have children trafficked for sexual exploitation, and to normalize and hide these crimes. We are pleased to see the ongoing international consensus to prioritize tackling this issue, including through a recent UN call to action on removing known child sexual exploitation and abuse material from the Internet.
- 27. We underscore that it is our individual and collective responsibility as governments and societies to do all we can to keep children safe from child sexual exploitation and abuse. In this regard, we remain committed to strengthening cooperation among the G7 and our partners and will continue to hold the perpetrators accountable using all the tools that our laws permit, proactively promoting and feeding into shared databases such as the International Child Sexual Exploitation database.



- 28. We acknowledge the strong role of victims' and survivors' voices and perspectives to inform our respective policy orientations, to help raise awareness of these crimes, and to support effective action in delivering future change and building appropriate safeguarding responses. We are committed to deepening our engagement with victims, survivors, and the organizations that work to support them going forward.
- 29. We recognize that it takes a whole-of-society effort, together with global action and standards to protect children from and fight against child sexual exploitation and abuse. We join the G7 Leaders in calling on the private sector to step up their efforts to identify and stop these crimes on their platforms. We stress the importance of each actor, including technology companies, taking all the steps they can to play their part in keeping children safe online around the world. We urge the ICT industry to further their cooperation with government, particularly with law enforcement agencies on information sharing, investigations, and reporting of online child sexual abuse material. We call on industry to take effective proactive action against child sexual exploitation and abuse, ensure that they do not inadvertently facilitate these crimes on their services, and that safety is prioritized at the design phase for the sake of countering serious threats and preventing harm to children, including by endorsing, and transparently implementing and reporting their progress on the Voluntary Principles to Counter Child Sexual Exploitation and Abuse. We reaffirm our commitment to the 2021 G7 Action plan to combat Child Sexual Exploitation and Abuse. We will continue to promote measures toward eliminating child sexual abuse materials on the Internet in close collaboration with the ICT industry, especially social media and other forms of online communication companies, along with civil society, including NGOs and wider international partners, as set out in Annex I.

VIII. Transnational Organized Crime

- 30. We affirm our joint effort to fight transnational organized crime in all its manifestations, including drug trafficking, firearms trafficking, trafficking in persons, migrant smuggling, child sexual exploitation and abuse, cybercrime, ransomware threats, crimes that affect the environment, corruption, fraud, intellectual property theft, copy right infringements, property crime, and money laundering. We further acknowledge that as transnational organized crime rapidly evolves, we need to better understand the linkages between different crime types and the tendency for illicit organizations to engage in polycriminality.
- 31. We affirm our commitment to various international cooperation frameworks (e.g. INTERPOL. Europol, the United Nations Office on Drugs and Crime), to continued engagement with other relevant international experts/bodies (e.g. civil society, academia), and to provide information and available resources. We acknowledge the need for law enforcement officials to continue to share information amongst themselves, investigate and build knowledge and capacity, especially on ICT, to adapt and respond to the evolving modus operandi employed by transnational organized crime networks and their engagement in polycriminality. Particularly regarding transnational organized fraud, we declare our enhancing cooperation in line with Annex II.
- 32. Given that proceeds of crime in digital and interconnected economies can be laundered quickly and transnationally, it is critically important to swiftly detect and freeze or seize the proceeds of crime at the earliest possible opportunity. This can be achieved only through close collaboration among relevant domestic and foreign authorities, international organizations such as



INTERPOL and its global stop payment mechanism, and the private sector including the financial and technology sector. In particular, being conscious of the fact that criminals are increasingly using digital assets to launder the proceeds of crime by taking advantage of their anonymous nature, we reaffirm our commitments through the international anti-money laundering mechanisms and reiterate the need to continue to develop rules and regulations to prevent criminal actors from exploiting our valuable economic infrastructure, and to prevent jurisdictional arbitrage by virtual asset providers. We support initiatives by the Financial Action Task Force (FATF) on accelerating global implementation of the FATF Standards on virtual assets, including the "travel rule," and its work on emerging risks. We endeavor to increase cooperation among the G7 members for freezing the digital assets transaction accounts and ensuring that mechanisms exist for the expeditious recovery of proceeds of crime that are digital assets, including through return to their lawful owners in appropriate cases, which includes sharing of information on digital assets transaction accounts (user accounts) that are being or suspected to be used for crime.

- 33. We recognize that corruption and the laundering of proceeds of crime obtained from corruption offences drains public resources, and often fuel organized crime. We reaffirm our will to work with our international partners in their fight against corruption, including cooperation in investigations, information sharing, and capacity building, to better prevent such acts and to hold corrupt actors accountable.
- 34. We also recognize the significant public health and security challenges posed by illicit drugs, including synthetic drugs, and other substances subject to misuse or abuse, as well as their negative impacts on societies. We will enhance efforts to target the illicit manufacturing and trafficking of these substances and related precursor chemicals, pursue and share information on criminals engaging in these activities, and disrupt the illicit supply chains at origin, transit, and destination points, while at the same time pursuing our efforts towards drug use prevention, treatment, and recovery services to minimize harms to people who use drugs. Working with implicated jurisdictions, we will also address the polycriminal dimension of drug trafficking, including the nexus between drug-related crimes and crimes that affect the environment, as well as firearms trafficking and money laundering. We will enhance our cooperation with other countries and international organizations through the Global Coalition to Address Synthetic Drug Threats and other multilateral fora.
- 35. We remain committed to preventing irregular migration whether by land, air or sea, which can result in tragic loss of life. We reaffirm our commitment to join efforts to tackle the organized criminal networks that profit off some of the most vulnerable by facilitating migrant smuggling and trafficking in persons and the dangerous journey of migrants and asylum seekers. We will intensify efforts to break the business model of organized criminal networks, including through further cooperation to disrupt the supply chains that enable the criminal and exploitative operations of those engaged in trafficking in persons and migrant smuggling.
- 36. We reaffirm our commitment to continue our international and transboundary cooperation to effectively prevent and combat crimes that affect the environment, including illegal transnational trafficking in wildlife such as protected flora and fauna, timber and timber products, hazardous and other waste, and precious metals, gemstones and other minerals, illegal mining, illegal logging, and crimes which could be associated with illegal unreported and unregulated fishing. We welcome the French initiative in organizing the first meetings of the network of experts on crimes that affect the environment this year.













- 37. We support and celebrate the central role INTERPOL plays in law enforcement cooperation between our nations in its centenary year and endorse INTERPOL's mission of delivering a safer world for all its members. We call for the organization to retain its focus on combatting international crime across INTERPOL's global remit, and that INTERPOL's future leadership ensure the organization continues to develop its global operational functions considering the growing international dimension across all spheres of criminal activity. We commit to continuing to support the organization in tackling the shared threats we now face.
- Annex I: G7 Call on Technology Companies to Take Actions to Fight against Online Child Sexual **Exploitation and Abuse**
- Annex II: G7 Declaration on Enhancing Cooperation in the Fight against Transnational Organized Fraud

