SECOND UNITED NATIONS HIGH-LEVEL CONFERENCE OF HEADS OF COUNTER-TERRORISM AGENCIES OF MEMBER STATES

TRANSFORMATIVE TECHNOLOGIES, SYSTEMS AND APPLICATIONS: TERRORISM-RELATED RISKS AND COUNTER-TERRORISM OPPORTUNITIES

1. **3D printing** may be defined as the action or process of making a physical object from a three-dimensional digital model, typically by laying down many thin layers of a material in succession. In 2019, the Wall Street Journal reported on an early example of the misuse of 3D printing technologies for terrorist purposes.[1] As 3D printing technologies advance and become increasingly accessible and affordable, they will present terrorists, including lone actors, with significant opportunities to carry out attacks using simple, lethal and hard-to-trace homemade guns.

2. **Artificial Intelligence (AI)** is a branch of computer science dealing with the simulation of intelligent behaviour in computers." [2] AI and AI-powered technologies[3] present significant potential to strengthen law enforcement capacities to identify objects or persons of interest, extract and analyse information from text-based sources, optimize law enforcement resources[4] and support the creation of "smart cities". [5] Using AI for law enforcement purposes raises serious human rights considerations, including with respect to privacy, data protection, and algorithmic bias. [6] AI also presents opportunities for terrorists to conceive and plan attacks, lower the financial and human costs of carrying out attacks, evade detection and conceal evidence. AI is enabling the programming of audio and video deep-fakes that could challenge identity verification and create impersonations to fuel conspiracy theories and hatred. [7]

3. **Autonomous weapons systems** cover a wide spectrum of potential weapons systems, including fully autonomous weapons that can launch attacks without any human involvement and semi-autonomous weapons that require affirmative human action to execute a mission. Advancing AI technologies and their increasing integration in autonomous weapons systems are anticipated to lead to more autonomous and far more dangerous weapons. [8]

4. **Biometric systems:** In its resolution 2396 (2017), the Security Council *"decides that* Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law."[9] Developing and maintaining such systems presents practical and legal challenges, including ensuring compliance with international human rights law. Member States should apply the Security Council Guiding Principles on Foreign Terrorist Fighters (Madrid Guiding Principles and its Addendum),[10] and may wish to consider the guidance provided in the United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism (2018) [11] and the University of Minnesota Human Rights Center report "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?", prepared under the

aegis of the mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. [12]

5. **Biotechnology:** The COVID-19 pandemic has highlighted global vulnerabilities to the possibility of bioterrorism. The United Nations Global Counter-Terrorism Strategy calls upon Member States, international organizations and the UN System to ensure that advances in biotechnology are not used for terrorist purposes; improve border and customs controls to prevent and detect illicit trafficking of biological, radiological and nuclear weapons and materials; and improve coordination in planning a response to a terrorist attack using chemical, biological, radiological and nuclear weapons or materials. In its resolution 1373 (2001), the UN Security Council specifically addressed the threat of chemical, biological, radiological and nuclear terrorism. It recognized the connection between international terrorism and, inter alia, the illegal movement of such materials. In its resolution 1540 (2004), the Council affirmed that the proliferation of chemical, biological, radiological and nuclear weapons and their means of delivery constitutes a threat to international peace and security.

6. **Internet and other media:** In the sixth review of the United Nations Global Counter-Terrorism Strategy (A/RES/72/284), Member States expressed "concern at the increasing use, in a globalized society, by terrorists and their supporters, of information and communications technologies, in particular the Internet and other media, and the use of such technologies, to commit, incite, recruit for, fund or plan terrorist acts." In its resolution 2396 (2017), the Security Council expressed concern that terrorists may craft distorted narratives to polarize local communities, recruit supporters and foreign terrorist fighters, mobilize resources, and win support from sympathizers, including through the Internet and social media. The Security Council Guiding Principles on Foreign Terrorist Fighters (Madrid Guiding Principles and its Addendum) provide guidance both for countering the use of the Internet for terrorist purposes and for collecting, handling, preserving and sharing information obtained from ICT for counter-terrorism purposes while protecting and protecting internationally protected human rights.[13]

7. **Internet anonymization services, virtual private networks (VPN), dark web, darknet, and end-to-end encrypted messengers:** Numerous encryption tools and anonymizing software are readily available online for download, and powerful end-to-end encryption technologies are now commonly embedded in electronic devices and online messaging apps. On personal computers, the de facto standard and freely available Pretty Good Privacy (PGP) software provide the same encryption grade used by the military to convert messages (or even entire files) into encrypted text that can be copy/pasted anywhere. Terrorists have exploited these technologies to communicate and store information, avoid detection and incrimination, and secretly plan terrorist attacks. While terrorists typically rely on open internet sources for recruitment and propaganda purposes, they are more likely to use encryption and the dark web for communications and transactions that lead to violent acts. *While end-to-end encryption itself often cannot be broken, intelligence agencies have been able to hack the software on the ends.* Technology companies, civil liberties advocates, and national government officials have widely argued that creating "backdoors" for law enforcement agencies to retrieve communications would do more harm than good.[14]

8. **Online gaming:** The online gaming industry has become one of the fastest-growing digital media segments. Terrorist groups have used online gaming to spread hate speech and terrorist content and groom and lure young recruits.[15] CTED's Tech Against Terrorism initiative researchers have identified how otherwise inoffensive online game creation systems have been misused by so-called right-wing extremists to recreate playable versions of infamous far-right atrocities, including Anders Breivik's 2011 attack on the Norwegian island of Utoya, the 2019 mosque shootings in Christchurch, New Zealand, and the 2019 terrorist attack in El Paso, Texas. Online games can also be used to encourage critical thinking and build resilience to misinformation, hate speech and terrorist narratives. The abilities of online games to build resilience to misinformation, hate speech and terrorism narratives may be short-lived, however, and should be complemented through a comprehensive educational approach.

9. **Unmanned aircraft systems (UAS)** ("drones") consist of an unmanned aircraft and its associated elements, including a remote pilot and a communication system between the two. While drones were initially developed for military use, advancing UAS technology has made it increasingly affordable and accessible for a wide range of uses. There have already been several examples of terrorists' use of weaponized UAS for surveillance, reconnaissance, propaganda and attacks. In addressing the potential risks posed by UAS, States should consider the potential impact that their responses could have on internationally protected human rights, especially when using UAS themselves.[16]

10. **Smart cities** may be defined as urban areas that use different types of electronic methods and sensors to collect data from citizens, devices, buildings and assets to gain insights to manage assets, resources and community services efficiently and improve operations across the city. Artificial Intelligence (AI) in "smart cities" can be used to autonomously detect, analyze and understand actions and events to improve, recognize and predict security threats in transportation hubs, infrastructures and sensitive locations. The CTED-UNOCT Compendium of Good Practices for the Protection of Critical Infrastructure Against Terrorist Attacks (2018) warns that "increased connectivity may also increase the attack surface and therefore expose critical infrastructure to a high risk of manipulation." Building more secure smart cities also presents essential human rights considerations, including privacy, data protection, algorithmic bias and non-discrimination.

11. **Virtual assets and payment systems:** In its resolution 2462 (2019), the Security Council “calls upon all States to enhance the traceability and transparency of financial transactions, in compliance with international law, including international human rights law and humanitarian law, including through assessing and addressing potential risks associated with virtual assets and as appropriate, the risks of new financial instruments, including but not limited to crowd-funding platforms, that may be abused for terrorist financing purposes and taking steps to ensure that providers of such assets are subject to anti-money laundering and countering the financing of terrorism (AML/CFT obligations).”[17] The Council encourages Member States to apply risk-based anti-money laundering and counter-terrorist financing regulations to virtual asset service providers and identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers.[18]

SOURCES CITED

[1] " Is 3-D Printing the Future of Terrorism," the Wall Street Journal, 25 October 2019, at: Is 3-D Printing the Future of Terrorism? - WSJ (last accessed 3 June 2021)
[2] Artificial Intelligence | Definition of Artificial Intelligence by Merriam-Webster.
[3] Relevant technologies, systems and applications include, for example (1) Algorithmic Filters, (2) Audio processing, (3) Autonomous weapons systems, (4) Data Airlock and Harmful Materials Recognition, (5) Fake videos or images ("Deep-fakes"), Major Events Screening and Surveillance (6), (7) Natural Language Processing, (8) Recommender System, (9) Resource Optimization (Law Enforcement), (10) Robotics, (11) Smart cities, (12) Smart policing, and (13) Visual processing.
[4] *Second INTERPOL-UNICRI Report On Artificial Intelligence For Law Enforcement* (2020) at UNICRI-INTERPOL_Report_Towards_Responsible_AI_Innovation_0.pdf
[5] For example, the Oslo Police District of Norway has been working with partners both within the police force, industry and academia to explore the application of A.I. to create more user-sensitive non-intrusive surveillance systems in smart cities. See: *Second INTERPOL-UNICRI Report On Artificial Intelligence For Law Enforcement* (2020) at UNICRI-INTERPOL_Report_Towards_Responsible_AI_Innovation_0.pdf
[6] *Second INTERPOL-UNICRI Report On Artificial Intelligence For Law Enforcement* (2020) at: UNICRI-INTERPOL_Report_Towards_Responsible_AI_Innovation_0.pdf, and General Recommendation No.36. Preventing and Combating Racial Profiling by Law Enforcement Officials (CERD/C/GC/36), 24 Nov 2020, at OHCHR | UN Committee issues recommendations to combat racial profiling
[7] *Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy: Report of the Secretary Genera*l (26 Feb 2020); and UNICRI-INTERPOL_Report_Towards_Responsible_AI_Innovation_0.pdf, page 11
[8] United Nations Security Council. Counter-terrorism Committee Executive Directorate: "Greater efforts needed to address the potential risks posed by terrorist use of unmanned aircraft systems: CTED Trends Alert," "(2019)
at: https://www.un.org/sc/ctc/wpcontent/uploads/2019/05/CTED-UAS-Trends-Alert-Final_17_May_2019.pdf
[9] (S/RES/2396 (2017), para. 15.
[10] Security Council Guiding Principles on Foreign Terrorist Fighters (S/2015/939 and S/2018/1177) at: Security-Council-Guiding-Principles-on-Foreign-Terrorist-Fighters.pdf
[11] United Nations Compendium of Recommended Practices For the Responsible Use & Sharing of Biometrics in Counter-Terrorism In association with the Biometrics Institute, (2018) at Microsoft Word - Compendium Final Draft June 18.docx
[12] *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business*?, University of Minnesota Human Rights Center (2019),
at: https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf
[13] International Covenant on Civil and Political Rights, esp. art. 19, para. 3
[14] Combating Terrorism Center at West Point: "How Terrorists use Encryption," "(June 2016), at Combating Terrorism Center at West Point (usma.edu)
[15] *Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy: Report of the Secretary-General*, 26 Feb 2020.

[16] *Greater Efforts Needed to Address the Potential Risks Posed by Terrorist Use of Unmanned Aircraft Systems: CTED Trends Alert* (2019), at CTED TRENDS ALERT (un.org)
[17] S/RES/2462 (2019) Para 20
[18] /RES/2462 (2019) Para 21