THEMATIC BRIEF: THE IMPACT OF THE WEAPONIZATION OF NEW TECHNOLOGIES AGAINST CIVIL SOCIETY

Prepared to Inform the Global Study on the Impact of Counterterrorism on Civil Society & Civic Space by the United Nations Special Rapporteur on the Promotion & Protection of Human Rights & Fundamental Freedoms While Countering Terrorism

Introduction

The development of new technologies promises enormously positive benefits for civil society, providing new possibilities for deepening connection and communication, promoting new educational and professional opportunities, and offering heightened security and efficiency. Those benefits, when distributed equally, transparently, and without discrimination, can make technology a partner in the strengthening of civil society and the promotion and protection of civil, political, economic, social and cultural rights for people worldwide. The various ways in which new technological capacities are being deployed in the name of counter-terrorism and P/CVE, however, represent a fundamental threat to protecting human rights, to civil society and meaningful civil society participation. This chapter builds on the Special Rapporteur's 2023 report to the Human Rights Council on the development, use and transfer of new technologies in the counter-terrorism and P/CVE context.[1] Drawing from the Global Study data, it surveys how the development and deployment of new technologies for counter-terrorism and P/CVE purposes—namely surveillance, content moderation, Internet shutdowns, biometrics and facial technology, and drones—have substantially limited the ability of civil society to exercise their fundamental rights and implement their core human rights, humanitarian, and other activities.

Surveillance

The capacity for mass surveillance as the default tool for counter-terrorism investigation has been dramatically increased by a series of converging trends in recent years: the precipitous decline in the cost of technology and data storage; the ubiquity of digital devices and connectivity; and the exponential increase in the processing power of computers. Calls by multilateral organizations to implement routine surveillance and data collection for counter-terrorism investigations have further incentivized the use and transfer of a range of hardware and software

[1] A/HRC/52/39.

tools.[2] Intrusion hardware takes many forms and functions to directly access physical communications infrastructure, such as the cables that carry worldwide Internet traffic, the servers of Internet service providers, or individual mobile devices.[3] Spyware software in particular infiltrates individual computers or mobile devices and can access and record video, audio, and text/email communications, including on supposedly secure platforms such as WhatsApp, as well as accessing calendars, contacts, and geolocation data. Spyware software has proliferated internationally and poses substantial risks to the promotion and protection of human rights. Such profound challenges have prompted legal inquiries and litigation worldwide.[4]

Issue in Focus: Surveillance Misuse
In August 2021, Special Procedures mandate-holders issued communications to the cyber-intelligence company NSO Group and Israel regarding the reported use of Pegasus spyware developed by the NSO Group to surveil, intimidate, and harass at least 180 journalists, human rights defenders and political leaders from 20 countries.[5]

The ubiquity of sophisticated communications surveillance poses obvious threats to civil society actors and organizations' rights of privacy and free expression, as well as related rights like the freedom of assembly, freedom of association, and freedom to manifest one's religion.[6] Many Global Study respondents, including Amnesty International,[7] reported experiences of digital surveillance of operatives or associates and transfer of their private data across Europe,[8] the Middle East,[9] Africa,[10] Latin America,[11] North America, and Asia & the Pacific,[12] leading to

[2] See, e.g., Council of Europe Cybercrime Programme Office, *Standard operating procedures for the collection, analysis and presentation of electronic evidence* (September 2019); INTERPOL, *Guidelines for Digital Forensics First Responders: Best practices for search and seizure of electronic and digital evidence* (March 2021).
[3] See, e.g., UK GCHQ Tempora program; US NSA XKeyscore and Upstream systems and Prism System; Russia System for Operative Investigative Activities. The operation of the Russian system was considered and held to constitute a breach of the European Convention right to privacy, by the Grand Chamber of the European Court of Human Rights in *Roman Zakharov v Russia* [2015] ECHR 1065; (2016) 63 EHRR 17.
[4] See, e.g., European Parliament, "Spyware: MEPs sound alarm on threat to democracy and demand reforms," press release committee of inquiry, 8 May 2023; European Parliament, *Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware* (2023); United States Federal Case No. 19-cv-07123-PJH, *WhatsApp Inc. et al v. NSO Group Technologies Ltd et al*.; A/HRC/51/16 (identifying additional hearings, investigations, criminal investigations, and civil lawsuits).
[5] AL ISR 7/2021.
[6] Fionnuala Ní Aoláin, *Position paper of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the Global Regulation of the Counter-Terrorism Spyware Technology Trade* (Spyware Position Paper) (2023), paras. 36-47.
[7] Amnesty International Input.
[8] See e.g., Central & Eastern Europe Consultation; Omnium Cultural Input; see also, e.g., A/HRC/52/34, para. 64; A/HRC/50/29, paras. 49-56.
[9] See Middle East & North Africa Consultation; see also, e.g., Access Now Input; Confidential Input (Occupied Palestinian Territory).
[10] See West, East, and Central Africa Consultation; see also, e.g., CIHRS Input.
[11] See Latin America & the Caribbean Consultation.
[12] See Asia & the Pacific Consultation.

concerns about covert data access, and, in a range of cases, to physical threats and violence facilitated by the pinpoint targeting spyware affords. In some cases, such surveillance has been entrenched or repurposed under cover of the Covid-19 pandemic and related regulations.[13] Such surveillance creates a chilling effect due to the *'very possibility'*[14] of surveillance—leading those most likely to be targeted (e.g., whistleblowers, political dissidents, journalists, human rights defenders) to self-censorship.[15] Multiple civil society organizations worldwide have opted to reduce or alter their strategies for communication and organizing so as to avert government scrutiny.[16]

The majority of surveillance tools have been obtained from private cybersecurity firms, including firms based in Israel, Germany, France, Italy, Hungary, North Macedonia, the United Kingdom, and the United Arab Emirates.[17] These businesses and multinational companies have benefitted from a dearth of regulation and due diligence, although the tide is shifting: for instance, in April 2022, Costa Rica became the first State to join the call for a moratorium on the trade in spyware technology,[18] while a broad coalition of civil society reiterated the demand for a moratorium at the World Economic Forum meeting, held in Davos, Switzerland, in May 2022.[19]

Content Moderation

Alongside the development of surveillance of *private* content, monitoring of *public* online content has also become widespread, prominently facilitated by new algorithmic and machine learning tools that allow for the efficient collection and analysis of social media posts, photographs, and private and professional networks as disclosed on publicly-accessible communications platforms. Recognizing that online media have been used to promulgate terrorist propaganda and hate speech,[20] civil society organizations have reported many instances where State agencies have invoked vague content moderation powers, including to prevent the promotion/glorification of terrorism, instead to block the communications of civil society actors.[21] Such impacts have been particularly keenly felt by those advocating on behalf of minority communities[22] or disseminating information

[13] See, e.g., Asia & the Pacific Consultation (Hong Kong).
[14] David Kaye, 'The Spyware State and the Prospects for Accountability' (2021) 27(4) *Global Governance* 483-492, 489.
[15] A/HRC/27/37, [20]; and A/HRC/32/38, [57].
[16] C&SN Input; West, East, and Central Africa Civil Society Consultation; Privacy International Input.
[17] A/HRC/52/39, para. 47.
[18] Access Now, "Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology," press release, 13 April 2022.
[19] Access Now, "Human rights leaders at Davos 2022: spyware is a weapon," press conference, 23 May 2022.
[20] UNDP Input.
[21] See, e.g., Coming Out Input; Access Now Input; Middle East & North Africa Consultation; Central & Eastern Europe Consultation.
[22] C&SN Input; Espacio Público Input; Access Now Input; Adalah (Israel) Input; EMR, CIHRS CFJ EFHR Input; NUPL Input.

perceived as critical of government.[23] Some States have also established information operations on social media to target civil society and smear them as terrorists, extremists, or sympathizers thereof.[24]
It is worth stressing that simply because content monitoring looks at *publicly-available* information, does not prevent it from being unlawfully intrusive.[25] As has been noted by the High Commissioner on Human Rights, the protection of the right to privacy extends to public spaces and information that is publicly available.[26] The Human Rights Committee has rejected the notion that data gathered in public areas is automatically in the public domain and may be freely accessed.[27]

Internet Shutdowns

States also deploy the blunt instrument of intentional Internet disruption as a public order mechanism purportedly in response to unrest—often under the pretext of counter-terrorism and national security.[28] Despite access to the Internet being widely recognized as an indispensable enabler of a broad range of human rights,[29] there were at least 182 Internet shutdowns in 34 countries in 2021 according to Access Now (compared to 159 shutdowns in 29 countries in 2020).[30] A relatively small number of countries are responsible for the vast majority of such disruptions: in 2021, there were 85 Internet shutdowns in Jammu and Kashmir and 15 shutdowns in Myanmar. The longest shutdowns have been a period from 2016 to 2021 in Pakistan's Federally Administered Tribal Area and 18 months in the Tigray region in Ethiopia. Trends reveal widespread use of mobile Internet shutdowns during protests in Bangladesh, Burkina Faso, Chad, Cuba, Eswatini, India, Indonesia, Iran, Iraq, Jordan, Kazakhstan, Myanmar, Pakistan, Senegal, South Sudan, Sudan, Turkmenistan, and Uganda, and during elections in 2021 in Chad, the Republic of Congo, Iran, Niger, Uganda, and Zambia.[31]

---

[23] See, e.g., Asia & the Pacific Input (Hong Kong, Myanmar, Indonesia; Singapore, Philippines, Vietnam, Thailand); Justice for All Input; MENA Rights Input
[24] See, e.g., Asia & the Pacific Input (Thailand).
[25] UNDP Input; ODIHR Input.
[26] A/HRC/39/29, para 6.
[27] CCPR/C/COL/CO/7 (Colombia), para. 32; European Court of Human Rights has also recognized that publicly available information may well fall within the scope of the right to privacy, especially when novel collection methods allow for the collation of a profile of an individual from disparate public sources, whereas each individual source of public information would not provide intrusive details. *Rotaru v Romania*, [43]; and *Vukota-Bojic v Switzerland*, [55].
[28] A/HRC/43/46/Add.1 para. 27 (Kazakhstan).
[29]A/HRC/RES/47/16; A/66/290, para. 12; A/HRC/50/55, paras. 7-14 (citing right to freedom of expression, the right to education, freedom of association and assembly, and the right to participate in social, cultural and political life, right to health, and the right to work and economic development).
[30] Access Now Database, "An Overview of Global Internet Shutdowns in 2022," Keep It On Database. Available from: https://www.accessnow.org/keepiton.
[31] The use of Internet shutdowns during election periods apparently to stymy opposition political organizing has previously been identified by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 'Freedom of Expression and Elections in the Digital Age,' Research Paper 1/2019 (June 2019).

The practical impact of Internet shutdowns on civil society and the role civil society organizations play in the expression and protection of human rights is catastrophic. As the 2022 OHCHR Report on Internet shutdowns records, shutdowns disrupt essential and emergency services in the health, education, and social assistance sectors,[32] with particularly acute effects for vulnerable or remote communities disproportionately reliant upon online access to services. The economic impact has also been catastrophic: the World Bank recently calculated that Internet shutdowns in Myanmar alone during 202 cost that country's economy nearly $2.8 billion.[33] Internet shutdowns also directly interfere with civil society organizations' primary channels of fundraising,[34] communication between staff, and dissemination of information to news outlets and the general public.[35]

Biometrics And Facial Recognition

Biometric surveillance technologies comprise a suite of tools including facial and gait recognition cameras and software which capture facial and/or movement characteristics, allowing for profiling of individuals on the basis of ethnicity, race, gender, and other apparent features, or even to identify specific individuals. Recognition technology is widely used to deal rapidly with large volumes of video footage and digital photographs, allowing users (typically law enforcement or security agencies) to process data efficiently and allocate resources away from initial identification. These systems have been controversially used for the profiling of persons as potential terrorist or extremist threats—using artificial intelligence algorithms which seek to predict individual behavior on the basis of datasets of previous behavior throughout the population. In addition, facial and gait recognition technologies are increasingly being integrated in counter-terrorism and P/CVE systems with artificial intelligence systems with the objective of identifying or inferring individual's intentions or emotions and, ultimately, predicting (and preventing) likely future conduct. Such recognition technologies

[32] A/HRC/50/55, paras. 35-39.
[33] World Bank Group, *Myanmar Economic Monitor: Contending with Constraints, Special Focus: Digital Disruptions and Economic Impacts* (2022).
[34] See, EMR, CIHRS, CFJ, EFHR Input.
[35] Coming Out Input.

are believed to have been used domestically in at least 64 countries,[36] and are particularly widespread in the United States,[37] United Kingdom,[38] and China.[39] Biometric monitoring tools raise significant human rights concerns. A system which necessarily requires the harvesting of biometric data from a large crowd without any discrimination between potential persons of interest and those raising no law enforcement interest inevitably casts its net too widely. As the High Commissioner for Human Rights has recommended, States should "[r]efrain from recording footage of assembly participants, unless there are concrete indications that participants are engaging in, or will engage in, serious criminal activity, and such recording is provided by law, with the necessary robust safeguards."[40] Disproportionate use of biometric monitoring has an inevitable chilling effect by which the fear of intrusive monitoring disincentivizes participation in civic events and so depopulates the public spaces which are the crucible of assembly, communications, protest movements, and democratic exchange.[41] That concern is particularly keenly felt by persons who already perceive themselves as targeted by State authority, including members of religious or ethnic minorities.[42]

Drones

The application of drones for counter-terrorism purposes also poses substantial risks for civil society. Drone technology is proliferating at a remarkable speed and has followed the same well-worn path from battlefield to the home front, which has been observed in policing tactics and weaponry generally. This move from use justified in the context of conflict and counter-terrorism to 'regular' homeland use tracks a consistent pattern where the exceptionality of counter-terrorism consistently moves to the local, domestic and 'regular' legal system.

---

[36] Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace Working Paper (September 2019); see also, e.g., Asia & the Pacific Consultation (Vietnam); Central & Eastern Europe Consultation (Hungary, Serbia). IRL 3/2022; OTH 229/2021 (European Union legislation: "A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond" and the Proposal for Amending Regulation (EU) 2016/794" on the use of artificial intelligence). Dr. Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* (Report 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).

[37] Police departments and defence agencies have all used the Clearview AI tool – a system which matches faces to a database of more than three billion images harvested from the Internet, including from social media platforms. See Katie Canales, 'Thousands of US Police Officers and Public Servants have Reportedly Used Clearview's Controversial Facial Recognition Tech Without Approval,' *Business Insider* (6 April 2021).

[38] As demonstrated in the first legal challenge to police facial recognition technology, police forces in the UK have deployed automated systems in crowd settings pursuant to ongoing trials since 2017. See *The Queen (on the application of Bridges) v Chief Constable of South Wales Police and ors* (2020) 1 WLR 5037 (CA).

[39] More than 100 cities operate such systems, and the central government is reported to be constructing the world's largest facial recognition database. See Jeffrey Ding, *Deciphering China's AI Dream*, Centre for the Governance of AI, Future Humanity Institute, University of Oxford (March 2018); CHN 18/2019 (collection of biometric data); CHN 14/2020.

[40] A/HRC/44/24, para. 53(i).

[41] Privacy International Input, referring to a forthcoming report from ECNL.

[42] A/HRC/32/38, para. 57; and A/HRC/29/32.

Particularly following the adoption in 2016 by the US Federal Aviation Authority of a rule permitting deployment of drones within domestic civilian airspace,[43] the use of drones by domestic law enforcement, first in the United States and then globally, has rapidly expanded[44] (including under the guise of enforcing the travel restrictions responding to the spread of the Covid-19 pandemic).[45] Police forces in the United States,[46] United Kingdom[47] and Europe, China, India, Israel, the Gulf, South America, and Australia are using these technologies.[48]
As drone technology becomes more sophisticated, it is likely that operators will shift to micro- or nano-drones, with profound human rights consequences resulting from their easier deployment and intrusion.

Issue in Focus: Technology Highlight
The Black Hornet drone— which weighs less than 20 grams, fits in one hand, flies virtually silently, and was developed by Prox Dynamics of Norway—is now officially used by approximately 20 military forces, including the United States Marines, the British Army and the armed forces of Australia, France, Germany, South Africa, Turkey and others. Current models can be equipped with cameras for motion and still images, with a 1.6 km range. Thousands of these micro-drones have been deployed by military forces in the past five years.[49]

The use of drones to surveil protests, and the unremarkable manner in which drone technology – once the exclusive preserve of covert battlefield operations – has, without proper regulation or scrutiny, become an everyday aspect of counter-terrorism and ordinary law enforcement tactics poses significant challenges for civil society operations. In addition to the obvious implications for privacy, freedom of assembly, freedom of expression and the like, the use of drones coupled with the coercive power of the police also risks violations of the prohibition on arbitrary detention, as well as the rights to liberty and security of the person, and the right to life.

---

[43] See, Federal Aviation Administration, *Timeline of Drone Integration*.
[44] See, e.g., Asia & the Pacific Input (Singapore); PEF Input; Central & Eastern Europe Consultation (Albania, Cyprus, Hungary).
[45] Privacy International Input, referring to the litigation brought by two French civil society organizations, La Quadrature du Net and La Ligue des Droits de l'Homme to block the use of drones to monitor Covid-19 regulation compliance in Paris.
[46] According to research, more than a thousand police departments in the United States are currently using drone technology. See Electronic Frontier Foundation, *Atlas of Surveillance Documenting Police Tech in Our Communities with Open Source Research*, Reynolds School of Journalism at the University of Nevada.
[47] At least 40 out of 43 police forces in the United Kingdom use drones. See: Chris Cole and Jonathan Cole, *Benchmarking police use of drones in the UK,* Drone Wars (2 November 2020). Not all forces publish details regarding their use of drones. Those which do include: West Midlands Police; Dorset Police; Lancashire Police; Sussex Police; and Kent Police.
[48] Christof Heyns, *Presentation made at the informal expert meeting organized by the States Parties to the Convention on Certain Conventional Weapons* 13-16 May 2014, Geneva, Switzerland, 13 May 2014.
[49] See, FLIR Wins Additional $15.4M Contract for Black Hornet Nano-UAV Systems for U.S. Army Soldier Borne Sensor Program, press release, 4 May 2021; FLIR Systems Awarded $89 Million Contract from French Armed Forces to Deliver Black Hornet Personal Reconnaissance System, press release, 18 January 2019; Government of Norway, Norwegian-developed drone to Ukraine, press release, 24 August 2022.

Recommendations

- **Address the development, use, and transfer of new technology** to surveil and by doing so curbing of civil society participation in communication, public discourse, and the exercise of their full human rights.
- **Commit to exercise legal powers governing the regulation or restriction** of information online in line with existing international human rights standards (including shutting down the Internet or blocking access to certain websites), exercising those powers only as necessary as part of a proportionate, necessary and non-discriminatory response to identified terror or security threats.
- **Ensure that, in their development, use, and transfer** of biometric technologies, including in the context of border management, they observe principles of legality, necessity, and proportionality.
- **Subject any proposed deployment of drones in domestic law enforcement contexts to close legal and judicial scrutiny** to ensure that the adverse human rights implications of widespread drone surveillance do not become normalized.
- **Address the disparate and discriminatory impacts** along race, age, and gender lines of the development, use and transfer of technologies for counter-terrorism purposes.