GLOBAL CENTRE
FOR THE RESPONSIBILITY
TO PROTECT

March 2024
POLICY BRIEF

The Relationship between Digital Technologies and Atrocity Prevention

New and emerging digital technologies — including, among others, social media platforms, artificial intelligence (AI), geospatial technology, facial recognition and surveillance tools — have and will continue to rapidly shift the space of human interaction in the modern world. As such, these technologies can both directly and indirectly impact how various actors may perpetrate or prevent mass atrocity crimes.

Digital technologies have, at times, been utilized to accelerate the spread of disinformation, generate information silos and target or dehumanize marginalized or persecuted groups, particularly ethnic or religious minorities. They have also been used to monitor populations and systematically restrict the work of civil society, human rights defenders and perceived government opponents, sometimes under the guise of serving counterterrorism purposes. Such technologies can also be crucial to the prevention of atrocities, for example, by enabling users to promote inclusive public discourse, document early warning signs of potential atrocities or amplify messages to compel international response.

Due to the rapid pace at which these technologies are developing, there is a notable gap in the capacity of multilateral institutions, including the United Nations (UN), individual states, regional organizations and private corporations to respond to the threat, as well as harness the potential of various digital technologies. While recent UN documents, such as the Strategy and Plan of Action on Hate Speech, the Secretary-General's report pursuant to Human Rights Council (HRC) Resolution 49/9 which has a particular focus on the impact of technological advances for genocide prevention efforts and the New Agenda for Peace, as well as the establishment of the Secretary-General's AI Advisory Body and several UN Security Council (UNSC) meetings on the linkages between various technologies and threats to international peace and security have brought increased attention to these new and emerging technologies, other resources, like the UN Framework of Analysis for Atrocity Crimes, lack this lens.

There is an increasing need to discuss how states and multilateral actors can harness the potential of new technologies as a tool for atrocity prevention, and aid in blocking those manipulating it for malignant purposes. This policy brief aims to examine the relationship between digital technologies and atrocity prevention, highlighting several technologies that may directly contribute to the perpetration and/or prevention of atrocities, and offers actionable recommendations for relevant stakeholders to address and mitigate the risks of emerging technology.

THE USE AND MISUSE OF DIGITAL TECHNOLOGIES

This brief will describe and assess how various technologies may increase the risk of mass atrocity crimes or serve as critical tools in preventing perpetration, strengthening human rights monitoring and facilitating justice and accountability. How these technologies are utilized, and by whom, greatly impacts their capacity to strengthen or degrade societal resilience to atrocities. The following section will assess a range of tools – from AI to geospatial and surveillance technologies – as well as mechanisms for influencing the use of technology – from misinformation campaigns to restricting internet access to vulnerable populations. The brief builds upon an event hosted by the Global Centre for the Responsibility to Protect and the European Union (EU) on 29 June 2023, during which experts discussed the linkages between digital technologies and atrocity prevention. The types of technologies and tools presented in this brief are therefore representative, rather than exhaustive.

Ralph Bunche Institute
for International Studies
CUNY Graduate Center
365 5th Ave., Suite 5203
New York, NY 10016 USA

info@globalr2p.org
T: +1 212-817-2104
F: +1 212-817-1565

www.globalr2p.org

Data Collection and Management

With the growing use of and access to digital technologies comes an increase in the volume of electronic data available to global actors that can be analyzed to find patterns and behavioral trends.[1] Through the collection of data, various state and non-state actors have immense access to information, intelligence sources and documentation capabilities.[2]

Data collection and management can pose risks for vulnerable populations, and potentially seriously undermine various human rights and freedoms, including the right to privacy.[3] As data collection tools become increasingly sophisticated and individual data is aggregated with little regulation and at the greatest possible scale, the risks associated with data mismanagement and cyber-attacks on critical data-collection infrastructure amplify.

Cyber-attacks can undermine information security and corrupt data-integrity, threatening the functioning of institutions, including UN and government entities. Worldwide such attacks have targeted critical civilian infrastructure, such as medical facilities, industrial control systems, nuclear power plants and complex supply chains.[4] This not only imposes excessive burdens on civilians by undermining the integrity and functioning of indispensable resources, but data collected from targeted breaches can potentially expose the identities of vulnerable people.

For example, the sensitive nature of health data collected by UN agencies, humanitarian actors and other nongovernmental organizations means that when a data leak or cyber-attack occurs, there can be serious security risks, particularly for survivors of mass killings or conflict-related sexual violence.[5] In addition, the possibility of data breaches may prevent survivors from seeking adequate medical attention, including out of fear that exposure will lead to stigmatization or further violence.

Data mismanagement poses significant risks to populations. Due to a lack of sufficient security protocols, the Kivu Security Tracker – a digital data collection project that tracked atrocities in eastern Democratic Republic of the Congo (DRC) – accidentally published personally identifiable and other sensitive information of up to 8,000 people, including activists, sexual assault survivors, UN staff, Congolese government officials, local journalists and victims of attacks.[6] In response to the breach, Daniel Fahey, a former coordinator of the UNSC-mandated Panel of Experts on DRC, said, "The database puts thousands of people and hundreds of organizations at risk of retaliatory violence, harassment, and reputational damage."

In some contexts, data collected on an individual's sexuality and gender has been reportedly used for surveillance, harassment, arrest and persecution by government officials.[7] LGBTQIA+ individuals often face specific vulnerabilities regarding the collection of individual data, particularly in countries with hostile policies or stigma that threaten their physical integrity.

However, big data presents new opportunities for human rights monitoring and accountability processes. When used responsibly, digital data collection tools increase the capacity of users to record information, maintaining and recognizing the rights and dignity of vulnerable individuals. Data disaggregation could be used to inform policymakers and advocates on the experiences of vulnerable populations to create more effective measures for inclusion in civic and public spaces, access to health and education, implementation of anti-discriminatory policies and practices, prevention of violence and access to justice.

National governments, regional organizations, UN entities and civil society can also harness big data and the open information environment to contribute to the investigation of international law violations, including atrocity crimes, in line with the Berkeley Protocol on Digital Open Source Investigations.[8] While the use of open source information in investigations is not new, the increasing sophistication of digital data collection tools have broadened the volume and diversity of open sources that can be submitted to international or national investigators. Moreover, digital information is less likely to be lost or destroyed so long as the integrity of the database remains intact.

Surveillance

The worldwide proliferation and misuse of increasingly sophisticated digital surveillance technologies has prompted concern regarding the capacity of this technology to facilitate human rights abuses and atrocity crimes.[9] The exponential growth in these technologies, much of which was originally justified by or intended for counterterrorism and national security purposes, has improved the capacity of state intelligence and law enforcement agencies to crack down on populations.[10]

China utilizes a comprehensive surveillance regime, including geospatial, biometric and cyber surveillance, among other strategies, both within and beyond its own borders, to facilitate identity-based abuses under the guise of combating religious extremism and terrorism. In August 2022 the Office of the UN High Commissioner for Human Rights warned in a report on the so-called Xinjiang Uyghur Autonomous Region (the Uyghur Region) that powers given to police and security forces, as well as domestic legislation on criminal procedure and counterterrorism, facilitate possible crimes against humanity and "provide legal underpinning for what has been alleged to be a sophisticated, large-scale and systematized surveillance system in practice, implemented across the entire region."[11]

Mass surveillance by Chinese authorities against Uyghurs and other predominantly Muslim and/or Turkic groups, has become a defining feature of government repression and ongoing persecution in the Uyghur Region.[12] The widespread use of facial recognition cameras and the forced collection of biometric data, as well as police checkpoints and the use of community informants, have turned the Uyghur Region into a de facto police state and are key instruments for facilitating atrocity crimes. The Chinese government also uses surveillance for transnational repression of Uyghurs around the world.[13]

The application of digital technologies in China's surveillance system also endangers refugees fleeing from the Democratic People's Republic of Korea (DPRK) through the Chinese border, the most common route for North Korean defectors. China uses surveillance technology to catch people crossing the border and facial recognition to identify foreigners who do not have state authorization.[14] Despite international protections, China considers border-crossers to be illegal "economic migrants," forbidding them from seeking asylum or resettlement, and deports them under a 1986 bilateral treaty with the DPRK. The forced repatriation of refugees and asylum seekers to the DPRK has left these populations at grave risk of internment, torture, sexual and gender-based violence, enforced disappearance or execution.

Geospatial technology

Geospatial technology refers to a wide range of location-based technologies that collect geolocated data, analyze patterns and deploy information.[15] In "black hole" environments, where information is deliberately hidden by local authorities or otherwise scarce, geospatial mapping may aid in accessing information.[16] However, the unlawful or invasive applications of geospatial technology are increasingly being used by perpetrators to monitor vulnerable populations and plan potential atrocities.

Geospatial technologies, including satellite imagery and some surveillance tools, have enabled dramatic advances in monitoring atrocity situations in so-called "black hole" environments. They offer increased intelligence capacity to track human rights violations and abuses, the movement of arms, the mobilization of armed groups or troops, the development or expansion of compounds, and the destruction of villages and mass movement of populations, among other things.

In the DPRK, pervasive censorship and information manipulation, as well as access constraints, have prohibited a complete assessment of the current human rights situation. Such widescale restrictions on access to information enables the authorities to reinforce prejudicial policies, incite further xenophobia and identity-based divisions and perpetrate widespread human rights violations and crimes against humanity with impunity.[17]

Geospatial technology can help circumvent information restrictions to gather evidence of potential atrocities. For example, while the DPRK authorities have denied the existence of political prisoner camps for decades, satellite images examined by the International Bar Association and the Committee for Human Rights in North Korea provide credible evidence of the precise location of camps for political prisoners, where between 80,000–130,000 people were detained as of June 2022.[18] These images not only confirm the existence of such camps and corroborate witness testimony, but also establish the exact location of several camps.[19] Similar investigations based on satellite imagery conducted have confirmed the existence of new detention sites in China's Uyghur Region in recent years, despite officials claiming that the reeducation camps had shrunk.[20]

Artificial Intelligence

The development of digital systems that can perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and translation and interpretation, forms the basis of AI.[21] The use of AI algorithms, systems and expertise, including predictive analytics and machine learning, artificial information and data collection, have become more widespread in recent years, posing both benefits for

prevention and risks for the perpetration of mass atrocities.

The UN Secretary-General's July 2023 report to the HRC on the impact of technological advances on genocide prevention efforts and on the risks of the perpetration of genocide notes that, "Predictive analytics and other forms of artificial intelligence are prone to reproducing and exacerbating biases reflected in existing algorithms, data and policies and leading to discrimination based on race, gender, religion, sexual orientation or nationality."[22] When coupled with repressive security sectors and/or state policies directly targeting populations on the basis of identity, this could increase disproportionate violence or detentions affecting certain groups within a society. It may also reinforce dangerous information silos and could greatly increase the capacity to incite violence, spread hate speech and disinformation on the basis of identity and weaken national resilience to atrocities, especially when engaged during triggering events like elections or other unique circumstances.

Due to the rapid development of AI, there is currently little legal regulatory oversight while the development of such systems is monopolized by a narrow set of non-governmental, private actors.

Malicious developers are known to use AI for disinformation campaigns and information warfare, including through the creation of "deepfakes," which generate human likeness and other characteristics. Disinformation campaigns that support actors implicated in grave crimes, when combined with other risk factors, can further embolden perpetrators.[23] In the context of the war in Ukraine, the EU identified artificial networks being created to spread disinformation relating to the Russian aggression, stating, "We have plenty of evidence that Russia is behind coordinated attempts to manipulate public debates in open societies."[24] This strategic application of AI contributes to an environment conducive for the commission of atrocity crimes.

AI can also be wielded as a tool for warfare, as image recognition systems can identify military objects by analyzing drone footage, as well as other intelligence streams, to recommend targets.[25] For example, the Israeli Defense Forces utilize an AI system named "the Gospel" to rapidly identify combatants and equipment, while purportedly minimizing civilian casualties.[26] However, such systems can also be used to deliberately target civilians and civilian objects with a sophisticated level of precision. Since 7 October 2023 Israeli air raids have targeted civilian objects protected under International Humanitarian Law, including residential buildings, hospitals, mosques, water and sanitation facilities, telecommunications towers, bakeries, schools and refugee and displacement camps across the Gaza Strip.[27] Israel's ability to substantially increase its targeting has resulted in an unprecedented number of civilian casualties and the widescale destruction of protected civilian objects in both Israel and Occupied Palestine.[28]

Nonetheless, opportunities for AI to contribute to atrocity prevention and response are expanding rapidly. AI and machine learning can positively aid human rights and humanitarian organizations by scanning, monitoring and analyzing public sources of data in atrocity situations. With further development, AI may also be able to monitor hate speech through machine-learning processes.[29]

AI-enabled data collection can recognize patterns on the ground to assess damage to civilian infrastructure, displacement, food security or the proliferation of weapons, among others.[30] This application may help to identify civilian protection needs, informing both humanitarian and peacekeeping operations that have civilian protection mandates. AI can further contribute to peacekeeping operations if integrated into monitoring and reporting activities. This includes data optimization and predictive tools for situational awareness, social media monitoring and behavioral analysis, as well as increasing security for sensitive data sets.[31]

Internet Access

UN Sustainable Development Goal 9.c establishes that access to universal and affordable internet is fundamental to building resilient infrastructure.[32] Equitable internet access enhances the realization of a broad range of human rights, including the rights to education, information, freedom of opinion and expression, among others.[33] However, control of internet access, through its intentional and arbitrary disruption, may be used as a tool to restrict human rights or to shield states from accountability.

Internet shutdowns are measures taken by a government, or on behalf of a government, to disrupt access to and the use of information and communications systems online.[34] Some internet shutdowns last several days or weeks, while others persist for months or years, often being imposed during moments of heightened tensions – such as public demonstrations or during electoral periods – armed conflicts or when governments carry out security operations. Shutdowns have been used to restrict civic space, including for human rights defenders and the

media, silence dissent and shroud human rights violations.[35] In the context of armed conflict and protests, internet shutdowns inhibit human rights reporting and monitoring, which often enables further violence, including grave human rights violations and possible atrocities, and helps avoid accountability.

Internet shutdowns also prevent civilians from sharing critical information regarding safety and medical access, among others, and contributes to impediments or delays in humanitarian assistance, endangering lives. In Myanmar (Burma), government-imposed internet shutdowns in areas where the military and ethnic armed groups clashed prevented civilians from receiving critical information regarding the COVID-19 pandemic and how to prevent its spread during 2020. Following the military's February 2021 coup, further restrictions in anti-military strongholds prompted a group of UN experts to condemn the country's "digital dictatorship."[36]

The government of Ethiopia has imposed at least 24 shutdowns since 2016.[37] According to Amnesty International, during a wave of demonstrations between June and October 2016 the Ethiopian government systematically and illegally blocked internet access to silence dissent and prevent reporting of attacks on protesters by security forces. Once the conflict in northern Ethiopia erupted during November 2020, the government effectively cut off internet access for six million people for two and a half years.[38] The barriers to internet access and lack of connectivity in many parts of Ethiopia made it challenging to document the full scope of violence in the Tigray, Afar and Amhara regions during the conflict and hindered the collection of evidence by human rights monitors of possible war crimes and crimes against humanity.

The capacity of civil society organizations, diaspora communities and human rights defenders to coordinate relief funds, monitor potential violations and share information depends upon connectivity with those in affected countries. After conflict broke out in Sudan in April 2023, human rights defenders were able to communicate early warning of atrocity risks in the Darfur region to global partners, helping to generate increased international attention and scrutiny at the time.[39] While access to the internet has since been restricted in Sudan, particularly in Darfur, the ability to share information online is vital to ensuring continued engagement and scrutiny from the international community.[40]

The use of digital evidence – such as emails, blogs, content on social media platforms and video and audio recordings – is becoming increasingly prevalent in international legal proceedings, including in prosecutions by the International Criminal Court (ICC) and in universal jurisdiction cases for war crimes committed in Syria and Iraq.[41] Arrest warrants were issued by the ICC for the abduction of Ukrainian children by Russian authorities from occupied areas of Ukraine, which was heavily supported by open-source intelligence and online information sharing.[42]

Social Media Platforms

Global access to social media and digital messaging platforms have been incredibly impactful in terms of our collective capacity to rapidly share information. Social media platforms have enabled diverse groups to connect and communicate, cultivating inclusive public discourse, compelling humanitarian responses and addressing early warning signs of potential atrocities. Social media can disseminate information quickly and provide a venue for underrepresented ethnic and minority groups to collaborate and raise awareness.

Social media platforms can also play a significant role in amplifying messages that dehumanize and ostracize specific groups as they create physical and mental distance and anonymity to perpetrators of hate speech. Hate speech and incitement to discrimination, hostility and violence are key early warning indicators of atrocities as such dangerous rhetoric is often a precursor, if not a prerequisite, for triggering violence, including atrocity crimes. The explosive growth of social media and digital messaging platforms have accelerated and contributed to the detrimental effects of information silos and disinformation and are increasingly used to contradict, distort or entirely deny past and ongoing atrocities or spread hateful messages that may influence or incite offline violence.

In the months and years prior to the 2017 Rohingya genocide, hate speech and anti-Rohingya content proliferated on Facebook in Myanmar. Several military actors and religious leaders spread anti-Muslim propaganda, including language that called for violence to be committed against the Rohingya. In 2018 the UN's Independent International Fact-Finding Mission (FFM) on Myanmar determined that social media, in particular Facebook, had played a "determining role" in the Rohingya genocide.[43] Facebook has continued to struggle with curbing hate speech and misinformation on the platform and the lack of effective content moderation has been further exploited by the junta since the military coup in 2021. Military authorities have also engaged in an online campaign, primarily through the messaging

platform Telegram, to intimidate democratic opposition and quash resistance efforts.

There are several relevant frameworks that can be applied to address, combat and prevent the risks posed by social media and digital platforms, including the UN Strategy and Plan of Action on Hate Speech, the Rabat Plan of Action and the Plan Of Action For Religious Leaders and Actors to Prevent Incitement to Violence That Could Lead to Atrocity Crimes, commonly referred to as the "Fez Process."[44] However, these strategies fail to comprehensively address all social media-related risks, particularly in a constantly evolving digital landscape. Likewise, states face difficulty in balancing their responsibility to address the risks posed by social media and digital platform usage, such as hate speech regulation and content moderation, and respect for fundamental freedoms, such as the rights to free speech and privacy. Gaps in the implementation of these strategies and the lack of long-term, meaningful engagement by states and social media companies, among other actors, further inhibits their effectiveness.

Social media platforms and technology companies have obligations to respond to and moderate disinformation, hate speech and incitement to violence on their platforms. Nonetheless, these companies have developed their own definitions of hate speech and measures to respond to it, which may not adequately address atrocity risk factors prevalent on their platforms or be in line with international human rights standards.

In contexts with state repression and/or widespread restrictions on fundamental rights and access to civic and public space, social media platforms can sometimes provide an important venue for spreading messages that are otherwise publicly stifled. In Venezuela, where the government has cracked down on civic space, social media provides an invaluable resource to civil society for gathering and sharing critical information. In instances where civil society organization offices were raided, and organization members faced arbitrary detention, social media platforms enabled others to coordinate an online campaign in support of those detained.[45]

Civil society in Venezuela, as well as in other countries, have also used social media to document human rights violations, advocate for victims' rights, access to appropriate medical, mental health and psycho-social support services and increase pressure on government authorities by raising awareness.[46] Several HRC-mandated investigative bodies, such as the FFM on Venezuela, the CoI on Syria and the CoI on Ukraine, utilize certified digital information, including social media content, as a method for data collection to establish and inform their findings.[47] The Independent Investigative Mechanism for Myanmar also uses open-source information, including user-generated content on social media platforms, to collect evidence of crimes, to corroborate information for other types of evidence, such as witness testimony, or to establish a connection between a perpetrator and a crime.[48]

RECOMMENDATIONS

For UN member states:

- Develop and strengthen norms and rules around the access and limitations of new and emerging digital technologies for both government and civilian use, including by establishing consultation mechanisms with civil society, private actors and other stakeholders.

- Ensure that the UN's Code of Conduct for information integrity on digital platforms is sensitive to social media-related atrocity risks and provides global response mechanisms that are grounded in atrocity prevention strategies.

- Review and, if necessary, strengthen domestic legislative and regulatory frameworks applicable to the digital industry, particularly social media providers, to prevent technology companies from facilitating the dissemination of hate speech and ensure that their services do not contribute to human rights abuses. Work with technology companies to identify, monitor and mitigate hate speech and misinformation and disinformation online.

- Develop national strategies on responsible design, development and use of emerging technologies, including geospatial and AI, facial recognition and surveillance tools.

- Agree on a global framework for the ethical use of data-driven technology and online services, including AI, to regulate and strengthen oversight mechanisms and ensure accountability for potential misuse.

- Establish authentication protocols for both international and domestic courts to respond to the increasing reliance on digital open-source material and to allow actors at every stage of the proceedings

ensure and assess the information's integrity and reliability.

- Ensure that addressing atrocity risks related to the use and development of AI systems are included on the agenda of the UN Secretary-General's High-level Advisory Body on Artificial Intelligence.

- Invest in national technology capacities that expand the usage and development of new technologies beyond the private sector, mitigating information asymmetry and the political leverage of the private sector which may influence any regulatory response.[49]

- Fully implement the commitments outlined in the Rabat Plan of Action and the Fez Process regarding incitement to violence on digital platforms.

- Request the UN Joint Office on Genocide Prevention and the Responsibility to Protect to incorporate risk factors posed by digital technologies in the Framework of Analysis for Atrocity Crimes.

- Impose restrictions on the sale or transfer of surveillance, geospatial and dual-use technologies to governments implicated in utilizing such tools to facilitate and perpetrate abuses.

For providers of technological services

- Pursue vigorous evaluation and testing of all new and emerging technologies prior to being released for general consumption.

- Ensure full compliance with human rights due diligence standards outlined in the Guiding Principles on Business and Human Rights, including in the management and moderation of social media platforms and in the development of AI and other enhanced-technological capacities.[50]

- Dedicate resources to content moderation, by hiring people who speak local languages and understand subnational and localized contexts, as well as atrocity prevention specialists.

- If possible to do so safely and responsibly, conduct regular outreach with marginalized groups and civil society to document and address concerns related to the technologies, such as on evolving hate speech forms/terms.

- Responsibly share digital evidence with independent investigative mechanisms and other accountability procedures, where applicable.

---

[1] Syed Iftikhar Hussain Shah, Vassilios Peristeras and Ioannis Magnisalis, "DaLiF: A data lifecycle framework for data-driven governments," *Journal of Big Data* vol. 8, no. 89 (2021), available at: https://doi.org/10.1186/s40537-021-00481-3.

[2] Federica D'Alessandra and Kirsty Sutherland, "The promise and challenges of new actors and new technologies in international justice," *Journal of International Criminal Justice*, vol. 19, no. 1 (2021), available at: https://doi.org/10.1093/jicj/mqab034.

[3] UN Human Rights Council, Resolution 42/15, A/HRC/RES/42/15, 26 September 2019.

[4] Eleonore Pauwels, "Peacekeeping in an era of converging technological & security threats," *UN Department of Peace Operations*, April 2021, available at: https://peacekeeping.un.org/sites/default/files/06_24_final_pauwels_converging_ai_cyberthreats_digital_peacekeeping_strategy_1.pdf.

[5] Kristin Bergtora Sandvik and Kjersti Lohne, "The struggle against sexual violence in conflict: Investigating the digital turn," *International Review of the Red Cross* (2021), available at: https://international-review.icrc.org/articles/struggle-against-sexual-violence-in-conflict-investigating-digital-turn-913.

[6] Robert Flummerfelt and Nick Turse, "Online atrocity database exposed thousands of vulnerable people in Congo" *The Intercept,* 17 November 2023, available at: https://theintercept.com/2023/11/17/congo-hrw-nyu-security-data/.

[7] UN Independent Expert on sexual orientation and gender identity, "Data collection and management as a means to create heightened awareness of violence and discrimination based on sexual orientation and gender identity," A/HRC/41/45, 14 May 2019.

[8] For more information on the Berkeley Protocol on Digital Open Source Investigations, see: https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source.

[9] UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism," A/HRC/52/39, 1 March 2023.

[10] UN Secretary-General, "Promotion and protection of human rights and fundamental freedoms while countering terrorism," A/69/397, 23 September 2014.

[11] UN Office of the High Commissioner for Human Rights, "Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China," 31 August 2022, available at: https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region.

[12] Global Centre for the Responsibility to Protect, "Global Centre for the Responsibility to Protect submission for the 45th session of the Universal Periodic Review Working Group in January 2024 concerning the People's Republic of China," 18 July 2023, available at: https://www.globalr2p.org/publications/submission-for-upr45-review-of-china/.

[13] David Tobin and Nyrola Elimä, "'We know you better than you know yourself:' China's transnational repression of the Uyghur diaspora," University of Sheffield, April 2023, available at: https://www.sheffield.ac.uk/seas/research/we-know-you-better-you-know-yourself-chinas-transnational-repression-uyghur-diaspora.

[14] Choe Sang-Hun, "For North Koreans in China, seeking freedom is more perilous than ever," *The New York Times,* 9 July 2023, available at: https://www.nytimes.com/2023/07/09/world/asia/north-korea-china-defectors.html.
[15] BAE Systems, Inc., "What is geospatial technology?," available at: https://www.baesystems.com/en-us/definition/what-is-geospatial-technology.
[16] Federica D'Alessandra and Kirsty Sutherland, "The promise and challenges of new actors and new technologies in international justice."
[17] UN Commission on Human Rights in the Democratic People's Republic of Korea, "Report of the commission of inquiry on human rights in the Democratic People's Republic of Korea," A/HRC/25/63, 7 February 2014.
[18] War Crimes Committee of the International Bar Association and the Committee for Human Rights in North Korea, "Inquiry on crimes against humanity in North Korean detention centers," June 2022, available at: https://www.ibanet.org/document?id=Inquiry-on-Crimes-Against-Humanity-in-North-Korean-Detention-Centers-2022.
[19] War Crimes Committee of the International Bar Association and the Committee for Human Rights in North Korea, "Inquiry on crimes against humanity in North Korean detention centers."
[20] Chris Buckley and Austin Ramzy, "Night images reveal many new detention sites in China's Xinjiang Region," *The New York Times,* 10 May 2021, available at: https://www.nytimes.com/2020/09/24/world/asia/china-cmuslims-xinjiang-detention.html.
[21] Milica Begovic, Alex Oprunenco and Lejla Sadiku, "Let's talk about artificial intelligence," United Nations Development Program, 13 March 2018, available at: https://www.undp.org/blog/lets-talk-about-artificial-intelligence.
[22] UN Secretary-General, "Impact of technological advances on prevention of genocide efforts and on the risks of the perpetration of genocide," A/HRC/53/45, 12 July 2023.
[23] Global Centre for the Responsibility to Protect, "Atrocity Alert No. 330: Ukraine, Burkina Faso and South Sudan," 11 January 2023, available at: https://www.globalr2p.org/publications/atrocity-alert-no-330/.
[24] Opening speech by Josep Borrell Fontelles, High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission at the EEAS Conference, "Beyond disinformation: EU responses to the threat of foreign information manipulation," 7 February 2023, available at: https://°www.eeas.europa.eu/eeas/disinformation-opening-speech-high-representativevice-president-josep-borrell-eeas-conference_en.
[25] International Committee of the Red Cross, "What you need to know about artificial intelligence in armed conflict," 6 October 2023, available at: https://www.icrc.org/en/document/what-you-need-know-about-artificial-intelligence-armed-conflict.
[26] Geoff Brumfiel, "Israel is using an AI system to find targets in Gaza. Experts say it's just the start," *NPR,* 14 December 2023, available at: https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st.
[27] Global Centre for the Responsibility to Protect, "Israel and the Occupied Palestinian Territory," 1 December 2023, available at: https://www.globalr2p.org/countries/israel-and-the-occupied-palestinian-territory/.
[28] Global Centre for the Responsibility to Protect, "Atrocities present, past and future – Escalating crimes and consequences in Israel and Occupied Palestine," 27 October 2023, available at: https://www.globalr2p.org/publications/atrocities-present-past-and-future-escalating-crimes-and-consequences-in-israel-and-occupied-palestine/; Yuval Abraham, "'A mass assassination factory:' Inside Israel's calculated bombing of Gaza," *+972 Magazine*, 30 November 2023, available at: https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/.
[29] The Sentinel Project, "Research summary document: Hatebase – AI for hate speech monitoring," 30 September 2022, available at: https://thesentinelproject.org/wp-content/uploads/2022/11/Hatebase-Using-AI-for-Hate-Speech-Monitoring. pdf.
[30] International Committee of the Red Cross, "Artificial intelligence and machine learning in armed conflict: A human-centred approach," 6 June 2019, available at: https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach.
[31] Eleonore Pauwels, "Peacekeeping in an era of converging technological & security threats."
[32] UN Department of Economic and Social Affairs, "Sustainable Development Goal 9: Targets and indicators," available at: https://sdgs.un.org/goals/goal9#targets_and_indicators.
[33] UN Human Rights Council, Resolution 47/16, A/HRC/RES/47/16, 26 July 2021.
[34] Office of the UN High Commissioner for Human Rights, "Internet shutdowns: Trends, causes, legal implications and impacts on a range of human rights," A/HRC/50/55, 13 May 2022.
[35] Office of the UN High Commissioner for Human Rights, "Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights."
[36] Office of the UN High Commissioner for Human Rights, "Myanmar: UN experts condemn military's "digital dictatorship," 7 June 2022, available at: https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship.
[37] Access Now, "Who is shutting down the internet in 2023? A mid-year update," 31 July 2023, available at: https://www.accessnow.org/publication/internet-shutdowns-in-2023-mid-year-update/.
[38] Access Now, "Open letter to the Ethiopian Government: Urgently end ongoing internet shutdowns in all regions across the country," 27 April 2023, available at: https://www.accessnow.org/press-release/open-letter-to-the-ethiopian-government/.
[39] Global Centre for the Responsibility to Protect, "Urgent alert on rising atrocity risks in Darfur, Sudan," 16 June 2023, available at: https://www.globalr2p.org/publications/urgent-alert-on-rising-atrocity-risks-in-darfur-sudan/.
[40] Mohammed Yusuf, "Report: Six African countries restricted internet access due to protests or political crisis," *Voice of America,* 28 July 2023, available at: https://www.voanews.com/a/report-six-african-countries-restricted-internet-access-due-to-protests-or-political-crisis/7202326.html.
[41] Karolina Aksamitowska, "Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands," *Journal of International Criminal Justice,* vol. 19, no. 1 (2021), available at: https://doi.org/10.1093/jicj/mqab035.
[42] International Criminal Court, "Situation in Ukraine: ICC judges issue arrest warrants against Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova," 17 March 2023; Conflict Observatory, "Russia's systematic program for the re-education and adoption of Ukraine's children," 14 February 2023, available at: https://hub.conflictobservatory.org/portal/apps/sites/#/home/pages/children-camps-1.
[43] UN Office of the High Commissioner for Human Rights, "Statement by Mr. Marzuki Darusman, Chairperson of the Independent International Fact-Finding Mission on Myanmar, at the 37th session of the Human Rights Council," 12 March 2018, available at: https://www.ohchr.org/en/statements/2018/03/statement-mr-marzuki-darusman-chairperson-independent-international-fact-finding.
[44] For more on the UN Strategy and Plan of Action on Hate Speech, see: https://www.un.org/en/genocideprevention/hate-speech-strategy.shtml. For more on the Rabat Plan of Action, see: https://www.istanbulprocess1618.info/rabat-plan-of-

action/. For more on the Plan Of Action For Religious Leaders and Actors to Prevent Incitement to Violence That Could Lead to Atrocity Crimes, see: https://www.un.org/en/genocideprevention/documents/Plan of Action Advanced Copy.pdf.

[45] "Joint NGO Letter: Standing in solidarity with Venezuelan human rights defenders," Global Centre for the Responsibility to Protect, 5 February 2021, available at: https://www.globalr2p.org/publications/joint-ngo-letter-standing-in-solidarity-with-venezuelan-human-rights-defenders/.

[46] Jasmine Garsd, "For many in Venezuela, social media is a matter of life and death," *NPR,* 11 September 2018, available at: https://www.npr.org/2018/09/11/643722787/for-many-in-venezuela-social-media-is-a-matter-of-life-and-death.

[47] UN Independent International Fact-Finding Mission on the Bolivarian Republic of Venezuela, "Report of the Independent International Fact-Finding Mission on the Bolivarian Republic of Venezuela," A/HRC/45/33, 25 September 2020; UN Independent International Commission of Inquiry on the Syrian Arab Republic, "Report of the Independent International Commission of Inquiry on the Syrian Arab Republic," A/HRC/54/58, 14 August 2023.

[48] For more information on the IIMM's use of open source investigations, see: https://iimm.un.org/faq/.

[49] American Progress, "How to regulate tech: A technology policy framework for online services," 16 November 2021, available at: https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/.

[50] For more information on the UN Guiding Principles on Business and Human Rights, see: https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights