11. International governance of artificial intelligence, cyberspace and outer space

Overview

Emerging and disruptive technologies such as artificial intelligence (AI), synthetic biology and quantum technologies are having a profound impact on security. Efforts to establish international principles of responsible use of these technologies are gathering pace. This chapter focuses on those efforts in three priority technology areas: AI, cyberspace and outer space.

It was an important year for the governance of AI at the international level in at least three respects (see section I). First, the group of governmental experts on autonomous weapon systems (AWS) under the 1981 Certain Conventional Weapons Convention (CCW) adopted language that could form the basis of a two-tiered regulation on AWS. The CCW also adopted a mandate that could mark a potential endpoint for the discussion on AWS in the context of the CCW. Simultaneously, states approved a new discussion track under the auspices of the United Nations General Assembly that could serve as a basis for a future ad hoc process to complement or replace the CCW process.

Second, states formally acknowledged the need to widen the conversation about AI risks beyond AWS, to cover other ways through which advances in AI may present challenges for international peace and security. This shift was reflected by the first-ever meeting of the UN Security Council on AI in July 2023 and the creation of two new discussion forums: the international summit on Responsible AI in the Military Domain (REAIM) and the AI Safety Summit.

Third, the conversations concomitantly reached deeper technical and higher political levels. At REAIM, for example, states extensively discussed the problems of transparency, interpretability and bias associated with the use of AI applications based on machine learning, while the AI Safety Summit led to extensive discussion and commitment to the testing and evaluation of advanced AI systems. At the same time, these discussions mobilized decision makers at much higher political levels than ever before. The UN secretary-general and several heads of state engaged personally on the issue. It was also notable that AI was a key point in the bilateral meeting between US President Joe Biden and China's President Xi Jinping in November 2023.

Information and communications technology (ICT) continued to play an active role in the foreign policy and military activities of states and other actors in 2023 (see section II). Cyber capabilities were often used in combination with other tools, mechanisms and activities. Cyber operations were a relevant dimension in wars in Ukraine and Gaza, with activity centring on distributed

denial of services (DDoS) attacks and website defacements, along with dis- and misinformation campaigns and influence operations. The Russian Federation's targeting of Ukraine's allies was another feature of cyber operations in 2023.

Outside of armed conflict there was a shift towards a greater use of cyber capabilities for longer-term intelligence-gathering with fewer large-scale or one-off operations. Some middle-power states increased the sophistication of their cyber espionage techniques and operations in 2023. Cybercrime and the use of surveillance software continued to affect individuals and organizations worldwide.

The geopolitical climate continued to challenge multilateralism as a means for developing additional norms or instruments for cyber governance, but there was progress within certain frameworks in 2023. Negotiations continued on a future UN cybercrime treaty despite concerns about its potential to negatively impact human rights; the Malabo Convention entered into force; European Union institutions drafted a Cyber Resilience Act; the International Criminal Court announced its intention to consider evidence on cyber misconduct; and there were multiple governmental and non-governmental initiatives focusing on specific cyber threats. This patchwork approach to cyber governance represents the most likely way forward but it will be important that initiatives incorporate accountability and transparency mechanisms.

Several multilateral initiatives for space security governance were also pursued at UN forums in 2023 (see section III). The UN Disarmament Commission adopted a consensus-based report on transparency and confidence-building measures (TCBMs) for outer space with practical recommendations for implementing TCBMs. Despite the decades-long stalemate in multilateral space security discussions, this demonstrated that agreement could be reached on smaller issues. However, at the UN open-ended working group (OEWG) on reducing space threats, which convened its final session in 2023, states were unable to reach consensus on a report. Nonetheless, these OEWG sessions highlighted key issues for upcoming discussions, including: ensuring the protection of civilians; preventing debris-creating anti-satellite weapons tests; regulating non-kinetic attacks on space systems; adopting measures for information-sharing; and clarifying the role of commercial entities in conflicts involving space systems. In November 2023 a UN group of governmental experts was convened to discuss further practical measures on prevention of an arms race in outer space, while the General Assembly proposed two new OEWGs.

The adoption of multiple UN processes risks further polarization and overlap of substance in discussions about space security governance. States will therefore need to participate in good faith, as well as dedicate efforts to ensuring complementarity and coordination to prevent further exacerbating the dynamics that underpin space security governance.

VINCENT BOULANIN, ALLISON PYTLAK AND NIVEDITA RAJU