United Nations A/79/224

General Assembly

Distr.: General
23 July 2024

Original: English

Seventy-ninth session
Item 97 of the provisional agenda*
Role of science and technology in the context of international security and disarmament

Current developments in science and technology and their potential impact on international security and disarmament efforts

Report of the Secretary-General

Summary

The present report provides an overview of scientific and technological developments of relevance to weapons, means or methods of warfare and their potential impact on international security and disarmament efforts, as well as developments in relevant intergovernmental forums, pursuant to General Assembly resolution 78/22. It covers artificial intelligence and autonomy, uncrewed systems, digital technologies, biology and chemistry, space and aerospace technologies, electromagnetic technologies and materials technologies. In addition, the convergence of technologies is addressed in the report.

* A/79/150.

24-13489 (E) 050824

I. Introduction

1. In paragraph 4 of its resolution 78/22 on the role of science and technology in the context of international security and disarmament, the General Assembly requested the Secretary-General to submit to the Assembly at its seventy-ninth session an updated report on current developments in science and technology and their potential impact on international security and disarmament efforts.

2. Science and technology contribute to human development and prosperity and are key enablers of efforts to implement the 2030 Agenda for Sustainable Development. As the Secretary-General noted in his policy brief on A New Agenda for Peace (A/77/CRP.1/Add.8), it is important to ensure that the steps taken to address the perils of weaponizing new and emerging technologies do not restrict access for countries of the global South to the huge benefits promised by such technologies for the advancement of the Sustainable Development Goals.

3. There are, however, continuing concerns that developments in science and technology of relevance to security and disarmament are outpacing the capacity of normative and governance frameworks to manage the risks. The benefits of new and emerging technologies cannot come at the expense of global security. Governance frameworks should be put into place in order to minimize harm and address the cross-cutting risks posed by fast-paced developments and converging technologies (ibid., action 11).

4. The present report provides an overview of scientific and technological developments of particular relevance to weapons, means or methods of warfare and their potential impact on international security and disarmament efforts, as well as developments in relevant intergovernmental forums.

II. Recent developments in science and technology of relevance to weapons, means or methods of warfare

A. Artificial intelligence and autonomy

5. Artificial intelligence systems can be integrated in a range of applications supporting military decision-making, planning and logistics, as well as enabling autonomy in weapon systems, potentially including autonomous functions to apply lethal force. The convergence of artificial intelligence with other domains of science and technology can create new pathways for the proliferation of weapons, and means and methods of warfare. Artificial intelligence developed for civilian purposes may be misused, including for political disinformation, cyberattacks, terrorism or other malicious purposes, which presents significant risks for dual-use technologies and international governance.

6. In addition to rapid advances in civilian artificial intelligence, there are increasing reports of use by States of artificial intelligence-enabled systems in a military context, and growing concern over the acquisition of such technology by non-State actors. While research and development of artificial intelligence is currently centred in a small number of States and primarily carried out by private sector actors, the intangible and fast-changing nature of the technology presents challenges for the monitoring, regulation and governance of the technology.

7. A particular concern is how to conduct rigorous testing that ensures the reliability, safety, security and accuracy of artificial intelligence systems in the military domain. Although there is general acceptance that artificial intelligence in the military domain should be “robust” (i.e. technically reliable and safe), the likely

differences between testing and deployment environments raise questions about how to ensure that robustness, including with regard to potential violations of international humanitarian law. For instance, when used for purposes such as target selection in autonomous weapon systems and decision support systems, artificial intelligence applications may pose a challenge to the principle of distinction as a result of, inter alia, data reliability issues, errors in pattern recognition and a lack of contextual understanding. When used to enable targeting on a large or indiscriminate scale, such applications may challenge the principles of proportionality and precaution.

8. The rapid advancement in generative artificial intelligence is an important development and underlines the scale of the data and computational resources that define contemporary artificial intelligence. Large language models represent a type of foundation model and are trained using broad data that can be adapted to a range of downstream tasks, including potential military uses. The rapid increase in the use of large language models and the release of open-source models that permit broader access present potential international peace and security risks, ranging from deliberate misuses aimed at creating novel weapons, means and methods of warfare, to a host of risks associated with military applications that can emerge even when the technology is used by responsible actors.[1] The trade-offs concerning transparency in artificial intelligence represent a significant current debate regarding the need to maintain a tradition of openness that can support innovation and development, and the need for oversight.

Relevant intergovernmental processes, bodies and instruments

9. At the 2023 Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, it was decided to continue the work of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. It was also decided that the Group should further consider and formulate, by consensus, a set of elements of an instrument, without prejudging its nature, and other possible measures to address emerging technologies in the area of lethal autonomous weapon systems, taking into account the example of existing Protocols within the Convention, proposals presented by high contracting parties and other options related to the normative and operational framework on emerging technologies in the area of lethal autonomous weapon systems, building upon the recommendations and conclusions of the Group, and bringing in expertise on legal, military and technological aspects. The Group considered that weapons systems based on emerging technologies in the area of lethal autonomous weapons systems rely on data sets that can perpetuate or amplify unintentional social bias, including gender and racial bias, and that can thus have implications for compliance with international law.

10. Although there are external initiatives, there is currently no intergovernmental process under the auspices of the United Nations that addresses the responsible life cycle of artificial intelligence in the military domain.

B. Uncrewed systems

11. Uncrewed systems can be piloted remotely, semi-autonomously or autonomously, and are employed in the aerial, ground and maritime domains. Uncrewed aerial systems remain the most common, although there has been growing development and use of maritime and ground systems. Applications of uncrewed

[1] The extent of the advantage offered by open-source models for potential malicious use is still being debated.

systems include military surveillance and reconnaissance, target acquisition and strike operations.

12. The versatility of uncrewed systems and their potential to reduce risk to the life of the operator compared with crewed equivalents make these systems increasingly attractive to both State and non-State actors. Uncrewed aerial vehicles, in particular, have found widespread use in conflict, as they are often cheaper and faster to produce than comparable crewed systems. Uncrewed systems can be either armed or unarmed. One example is loitering munitions, which are one-way attack aerial system that combine characteristics of uncrewed aerial systems and missiles, whereby the system itself is used as the weapon, loitering in the air until it strikes. The recent use of uncrewed systems in populated areas has raised concerns regarding the protection of civilians and compliance with international humanitarian law, including by enabling strikes, on a large scale, against targets far removed from the front line. Moreover, the use of armed uncrewed systems risks lowering the threshold for the use of force, owing in part to the lower perceived risk to the human operator.

13. Scientific and technological developments are aimed at enhancing the performance of the individual components comprising uncrewed systems, as well as the systems as a whole, with a view to improving their endurance, reliability and performance.[2] However, uncrewed systems are vulnerable to interference, including the jamming or spoofing of surveillance data, communications and positioning systems. Integration of artificial intelligence is one method whereby autonomy could be increased and reliance on potentially vulnerable communication links could be reduced (see also sects. II.A and II.F).

Relevant intergovernmental processes, bodies and instruments

14. In its resolution 2370 (2017), the Security Council strongly condemned the continued flow of weapons, including unmanned aircraft systems and their components, to and between illegal armed groups, terrorists and other unauthorized recipients and encouraged Member States to prevent and disrupt procurement networks for such weapons, systems and components. The Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes was adopted in 2022.[3] In 2023, the Abu Dhabi Guiding Principles on uncrewed aerial systems were prepared in accordance with that Declaration (see S/2023/1035).

15. Regarding the improvement of transparency in armaments and the promotion of responsible transfers, uncrewed systems are explicitly included in category IV ("Combat aircraft and unmanned combat aerial vehicles") and category V ("Attack helicopters and rotary-wing unmanned combat aerial vehicles") of the United Nations Register of Conventional Arms. Some States parties to the Arms Trade Treaty have included uncrewed systems in their reports submitted pursuant to the Treaty.

C. Digital technologies

16. Increasing reliance on and advances in digital technologies continue at a rapid pace. The growth of the Internet of things continues unabated, with an estimated 7 billion connected devices and that number expected to increase to 22 billion by 2025.[4] Breakthroughs in digital technologies, including information and communications technologies (ICTs), quantum technologies, cloud computing, blockchain

[2] United Nations Institute for Disarmament Research (UNIDIR), "Uncrewed aerial, ground, and maritime systems: a compendium", April 2023.

[3] See https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/outcome_document_ctc_special_mtg_final_e.pdf.

[4] See https://www.oracle.com/internet-of-things/what-is-iot/.

technologies, 5G networks and artificial intelligence, continue to present opportunities for transforming industries, economies and societies.

17. The expanded use of digital technologies offers unparalleled opportunities for societies. However, the exploitation of new vulnerabilities and the malicious use of such technologies could have implications for international peace and security. Malicious activity could have cascading effects at the subregional, regional and global levels. Beyond the direct effects on the population resulting from the impact on critical infrastructure, malicious activity utilizing digital technologies can also undermine trust and confidence in electoral processes and public institutions, while also affecting the confidentiality, integrity and availability of data.

Information and communications technologies

18. Malicious use of ICTs by both State and non-State actors is on the rise. In 2023, serious incidents were reported, including those with an impact on infrastructure that provides essential services to the public, such as health care, banking and civilian telecommunications. Exploitation of software vulnerabilities, including through commercial sale of information about those vulnerabilities over the Internet, also continued.

19. Over the past year, some States have reported a significant increase in incidents involving ransomware, noting rising criminal, financially motivated activity.[5] According to some estimates, total ransomware payments reached a record high of $1.1 billion in 2023.[6] Proliferation of various types of malicious software, such as malware, wipers and trojans, combined with an expansion of techniques, such as spear phishing, cloud exploitation and distributed denial-of-service attacks, also continued to be well documented across regions and with varying levels of impact. There was growing concern over the proliferation of commercially available cyberintrusion capabilities, including spyware and other "exploitation kits".[7] Malicious activity targeting supply chains of companies such as software providers was also reported to have had disruptive effects.[8]

20. A diversification of actors and techniques continued to complicate the threat landscape. Non-State actors, including criminal organizations, terrorists, hacker groups and individuals, utilized various tools, techniques, exploits and attack vectors to cause disruption and destruction to networks, applications and content.

Quantum technologies

21. States have increasingly drawn attention to the potential implications of novel quantum technologies for international peace and security. The integration of quantum properties into applications such as computation, communication, sensing and imaging, and cryptography can have a considerable enabling and transformative impact, including for international peace and security. For example, quantum computers will allow for exponentially higher computing speeds and an ability to solve problems of higher complexity. Quantum sensing and imaging allow for the

[5] See https://www.cisa.gov/stopransomware/official-alerts-statements-cisa.

[6] Alexander Culafi, "Chainalysis: 2023 a 'watershed' year for ransomware", TechTarget, 7 February 2024.

[7] See https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities.

[8] Karamveer Singh Sidhu, "Top 5 famous software supply chain attacks in 2023", CloudSEK, 24 November 2023.

capture of objects with a resolution beyond what is possible with classical sensor technologies, while post-quantum cryptography is considered highly secure.

22. However, in addition to those potential benefits, quantum technologies pose potential risks to international peace and security. For instance, quantum computing is expected to challenge current cryptographic systems, making digital infrastructure, including infrastructure that provides essential services to the public, vulnerable to malicious targeting and activities. Also noteworthy is a potential increase in "harvest now, decrypt later" attacks, whereby malicious actors accumulate sensitive, encrypted data, cognizant that technology will facilitate decryption at a later date.

23. While the impact of quantum technologies is expected to be far-reaching, currently fewer than 20 countries have invested in a national programme of related research and development. In order to avoid a deepening technological divide, a commitment to inclusivity in quantum education is therefore important.

5G networks

24. The increasing ubiquitousness of the fifth generation of cellular technology, known as 5G, is revolutionizing communications with the potential for considerably faster download and upload speeds, as well as reducing the time required for communication between connected devices. While the transition to 5G technology continues, new opportunities and vulnerabilities have emerged. This technology has been hailed as providing an array of benefits, such as enhanced connectivity for smart cities, telemedicine and overall economic growth. However, risks have also been identified, such as the malicious or inadvertent introduction of vulnerabilities at the design stage. There is also the possibility of introduction or emergence of vulnerabilities in the supply chain and related 5G architecture.

Relevant intergovernmental processes, bodies and instruments

25. Developments in the field of information and telecommunications in the context of international security have been on the agenda of the General Assembly since 1998.[9] Discussions in expert groups and open-ended working groups have resulted in recommendations on norms, rules and principles for the responsible behaviour of States, and confidence-building and capacity-building measures, and there has been discussion on how international law applies to the use of such technologies (see A/65/201, A/68/98, A/70/174 and A/76/135). In parallel to the work of the sixth Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, an open-ended working group on developments in the field of information and telecommunications in the context of international security was established by the General Assembly in its resolution 73/27. The Group adopted a consensus report in March 2021 (A/75/816), which was endorsed by the General Assembly in its decision 75/564.

26. In 2020, the General Assembly established a second open-ended working group on security of and in the use of information and communications technologies with a five-year mandate to, inter alia, further develop the rules, norms and principles of responsible behaviour of States; continue to study existing and potential threats in the sphere of information security and how international law applies to the use of ICTs by States; and consider confidence-building measures and capacity-building. The working group adopted its first progress report in July 2022 (A/77/275) and a second one in 2023 (A/78/265) containing a number of recommended next steps, including the establishment of a global, intergovernmental points of contact directory. In those

[9] For more information on intergovernmental deliberations on developments in the field of information and telecommunications in the context of international security, see www.un.org/disarmament/ict-security.

reports, the “gender digital divide” was recognized and the need for gender-responsive capacity-building efforts was affirmed.

27. Under the auspices of the open-ended working group, States have continued to consider existing and emerging threats to the security of ICTs. States have variously reflected on the impact of digital technologies on international peace and security, including ICTs, artificial intelligence and quantum technologies, including consequences of convergence between and among them.

D. Biology and chemistry

28. The norm against the hostile uses of chemistry and biology is long-standing and enshrined in international law through the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction of 1972 and the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction of 1993. However, recent uses of chemicals as weapons, allegations of the development of biological weapons, and advances in chemistry and biology threaten to undermine these legal and normative measures.

29. Advances in biology and chemistry are accelerating and becoming increasingly interconnected. In general, such advances present a number of opportunities to address societal challenges. However, they can also pose risks to international peace and security.

30. The approval of a gene-editing therapy using clustered regularly interspaced short palindromic repeats (CRISPR) to treat sickle cell disease and transfusion-dependent beta thalassaemia has demonstrated the potential of such technology in helping to cure previously untreatable conditions.[10] However, the power to edit genes also brings with it significant risks. Theoretically, the same techniques could be misused to enhance agents used in past biological weapons programmes or create new forms of biological weapons. Such misuses call for robust governance, international collaboration and dedicated research into the unintended effects of gene editing to ensure that these innovations benefit humanity without posing undue risks.

31. The commencement of human trials of neural interface technology has brought closer the blending of human cognition with machines. In 2024, the first human implant of a neural interface by a private company was performed. The prospects for medicine are exciting, with the potential of restoring lost sensory functions or helping to treat brain disorders. However, the implications for security could be profound. The technology could be exploited to manipulate or control human behaviours, therefore reinforcing the need for strict ethical standards and protective measures.[11]

32. Both fixed-wing and rotary drones are being used to monitor crops and livestock, as well as to deliver nutrients and pesticides to crops in an intelligent, efficient manner that maximizes output. In law enforcement, semi-autonomous drones that can disseminate riot control agents to affect crowds of people have been developed. The potential malicious use of agricultural and riot control drones as carriers of harmful agents is an ongoing concern, especially as they become more affordable and widespread.

[10] Cormac Sheridan, “The world’s first CRISPR therapy is approved: who will receive it?”, *Nature Biotechnology*, vol. 42, No. 1 (January 2024); Willow Shah-Neville, “A gene editing milestone: the FDA approves CASGEVY, the first CRISPR-based therapy”, Labiotech, 11 December 2023.

[11] Miryam Naddaf, “Mind-reading devices are revealing the brain’s secrets”, *Nature*, vol. 626, No. 8000 (February 2024); Rachael Levy, Marisa Taylor and Akriti Sharma, “Elon Musk’s Neuralink wins FDA approval for human study of brain implants”, Reuters, 26 May 2023.

33. The integration of new technologies is also leading to innovative treatments and countermeasures against biological and chemical threats, such as antidotes to poisons and new countermeasures to nerve agent exposure.[12] Such developments are vital for enhancing resilience against, and even dissuading, potential attacks.

Relevant intergovernmental processes, bodies and instruments

34. Both the Biological Weapons Convention and the Chemical Weapons Convention have provisions for review conferences every five years, at which relevant scientific and technological developments are reviewed. The ninth Review Conference of the States Parties to the Biological Weapons Convention was held in November and December 2022, and the fifth Review Conference of the States Parties to the Chemical Weapons Convention was held in May 2023.

35. Both treaties contain provisions relating to more regular means of reviewing relevant developments in science and technology. Pursuant to a mandate from the Conference of the States Parties to the Chemical Weapons Convention, the Director General of the Organisation for the Prohibition of Chemical Weapons (OPCW) established a Scientific Advisory Board within OPCW. In 2023, the Board convened its thirty-seventh session,[13] and its temporary working group on the analysis of biotoxins concluded its work and issued its end-of-mandate report.[14] In addition, the Board issued a comprehensive scientific report on advancements in science and technology in support of the fifth Review Conference of the States Parties to the Chemical Weapons Convention.[15] Furthermore, OPCW has inaugurated its Centre for Chemistry and Technology, which will enable it to carry out research activities to support and strengthen the verification regime, and to conduct training courses and other capacity-building activities.

36. At the ninth Review Conference of the States Parties to the Biological Weapons Convention, in 2022, States parties agreed to establish a working group on the strengthening of the Convention. The mandate of the working group is to identify, examine and develop specific and effective measures, including possible legally binding measures, and to make recommendations to strengthen and institutionalize the Convention. Part of the mandate is to discuss scientific and technological developments relevant to the Convention and recommendations for the establishment of a mechanism to review and assess such developments and to provide advice to States parties. Discussions on these topics took place at the second session of the working group, in August 2023, and will continue through intersessional work and future meetings ahead of the tenth Review Conference, to be held in 2027.

E. Space and aerospace technologies

Missile technologies

37. Developments in emerging technologies are enabling new and expanded functions of missile systems, which are increasingly used as long-range strike weapons in armed conflict. These developments have implications for international

[12] Illia V. Kapitanov and others, “Sustainable ionic liquids-based molecular platforms for designing acetylcholinesterase reactivators” *Chemico-Biological Interactions*, vol. 385 (November 2023).

[13] OPCW, “Report of the Scientific Advisory Board at its thirty-seventh session”, document SAB-37/1.

[14] OPCW, “Analysis of biotoxins: report of the Scientific Advisory Board’s temporary working group”, document SAB/REP/1/23.

[15] OPCW, “Report by the Director-General: report of the Scientific Advisory Board on developments in science and technology to the Fifth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention”, document RC-5/DG.1.

peace and security and efforts to ensure disarmament, the effective regulation of arms, non-proliferation and respect for humanitarian principles.

Ballistic missiles and artillery rockets

38. A growing number of States are pursuing various technological innovations that have increased the accuracy of ballistic missiles and artillery rocket systems. This has enabled the use of longer-range ballistic missiles and rockets as strike weapons, including in ongoing armed conflicts and other high-profile incidents. Some non-State actors have also been able to acquire and use ballistic missiles and rockets.

39. These technological innovations have also enabled the development and testing of large-calibre artillery rocket systems that may blur distinctions between artillery rockets and ballistic missiles capable of delivering a nuclear weapon. That trend has continued to pose a challenge to regimes designed to curb the proliferation of ballistic missiles capable of delivering nuclear weapons.

40. These developments have also led States to develop and acquire missile defences, some types of which can exacerbate tensions and increase instability, in the light of different views on the relationship between offensive and defensive weapon systems.

Hypersonic glide vehicles

41. Some States have also continued to develop and deploy missiles equipped with warheads that can glide and manoeuvre at hypersonic speeds over long distances within the atmosphere, sustained by aerodynamic lift. Hypersonic glide vehicles could be capable of avoiding mid-course missile defences and challenging terminal defences, owing to their manoeuvrability or because they fly below the horizon for terminal defence radars at distances farther from their targets. The use of these systems has not yet been observed in armed conflict, and the strategic implications are not fully understood. Nonetheless, the first known deployment in 2019 of a hypersonic glide vehicle on an intercontinental-range ballistic missile sparked concerns over a new strategic arms competition.

Powered hypersonic vehicles

42. States and private companies have continued to test scramjet engines designed at least in part to enable hypersonic cruise missiles that are more capable of evading air defence and anti-missile systems. Such systems in active development may be capable of being launched by ground-, sea- and aircraft-based boosters and armed with conventional or possibly nuclear warheads.

Anti-missile and terrestrial anti-satellite systems

43. More States are developing and acquiring anti-missile systems, including in direct response to their use in ongoing armed conflicts. Surface-to-air systems that intercept their target within the lower atmosphere are increasingly common. The widespread deployment of these systems has resulted in greater acquisition and use of inexpensive self-detonating drones, including in attempts to overcome such defences.

44. States have continued to develop, test and deploy anti-missile systems designed to strike missiles outside the atmosphere in the mid-course phase of flight. The more capable of those systems have a de facto ability to strike satellites in low Earth orbit. States also continue to deploy terrestrial missiles that have reportedly been developed specifically to strike satellites in low Earth and geostationary orbit.

Relevant intergovernmental processes, bodies and instruments

45. The General Assembly established three panels of governmental experts on the issue of missiles in all its aspects between 2001 and 2008 (see A/57/229, A/61/168 and A/63/176). Although the issue of missiles remains on the agenda of the First Committee, there has been no resolution on the topic since the adoption of resolution 63/55.

46. There are two intergovernmental arrangements comprised of voluntary measures dedicated to missile technology. The Missile Technology Control Regime was established in 1987 with the aim of limiting the spread of ballistic missiles and other uncrewed delivery vehicles capable of delivering weapons of mass destruction. It has 35 members. The Hague Code of Conduct against Ballistic Missile Proliferation, adopted in 2002, includes politically binding commitments by States to exercise maximum restraint in developing, testing and deploying ballistic missiles and to uphold transparency measures regarding policies on, and launches of, ballistic missiles and space launch vehicles. A total of 145 States subscribe to the Code.

47. The issue of terrestrial anti-satellite weapons has been raised in various United Nations bodies concerned with outer space security, including most recently in the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space. The General Assembly, in its resolution 77/41, called upon all States to commit not to conduct destructive direct-ascent anti-satellite missile tests.

Space-based technologies

48. Military forces are increasingly dependent on space-based technologies for tasks such as early warning, navigation, surveillance, targeting and communications. Space systems, including satellites, are particularly vulnerable to various counter-space capabilities.

Capabilities used in rendezvous and proximity operations

49. Many emerging capabilities entail rendezvous and proximity operations, involving satellites that manoeuvre closely to a target satellite in order to operate nearby or to make physical contact. Beyond their beneficial applications, such as satellite maintenance and repair, such operations could also be used for non-consensual, risky, disruptive or hostile acts.

50. Development has continued on systems that can provide other services to active satellites in orbit, including inspection, repair, augmentation and relocation. Commercial companies first demonstrated in 2020 the launch of a satellite capable of docking with and extending the life of a target satellite that had exhausted its fuel supply.

51. An increasing number of commercial companies have deployed so-called space tugs, designed for the deployment of multiple payloads to precise orbits at different orbital planes and altitudes. These systems are designed to manoeuvre after orbital insertion and deploy many small satellites at different points over the course of their trajectories. Some satellites have been observed deploying small secondary payloads at relatively high velocities.

52. Commercial companies have continued to launch technology demonstration satellites in support of the development of active debris removal capabilities. These companies continue to study various means, including the use of robotic arms, nets, harpoons, magnets and adhesives, as well as the possible use of space-based lasers to destroy relatively small-scale space debris.

53. A number of States have continued to launch and operate satellites designed to visually inspect the satellites of others, especially in the geostationary belt. These have generally involved systems operated by military or national intelligence agencies and have approached both commercial and other military satellites.

Other space-based capabilities

54. Commercial companies have also demonstrated the capability of incorporating heat shielding onto their satellite payloads in order to retrieve materials that have been manufactured in orbit. Commercial actors have recently developed and used re-entry systems for crewed spacecraft, although States have relied on such technologies for decades.

55. States and commercial companies have continued to study and test space-based lasers for means of communications. While lasers with low power can potentially dazzle or temporarily blind optical sensors, higher-power lasers can damage certain sensitive components of satellites or other space-based systems.

Relevant intergovernmental processes, bodies and instruments

56. International law prohibits the placement and installation of nuclear weapons or any other weapons of mass destruction in orbit or on celestial bodies or the stationing of such weapons in outer space in any other manner; the establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies; and any nuclear weapon test explosion, or any other nuclear explosion, in outer space.[16]

57. The prevention of an arms race in outer space has been on the agenda of the Conference on Disarmament since 1985.

58. The Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities agreed on a consensus report in 2013 (A/68/189). In 2023, the Disarmament Commission agreed to a recommendation on the practical implementation of the recommendations contained in the Group's report (see A/78/42). In 2019, the Committee on the Peaceful Uses of Outer Space adopted the preamble and 21 guidelines for the long-term sustainability of outer space activities (A/AC.105/C.1/L.366), subsequently re-establishing the Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee with a five-year plan, which commenced in 2021.

59. At the request of the General Assembly, in recent years the Secretary-General established two groups of governmental experts on further practical measures for the prevention of an arms race in outer space. The Group established pursuant to resolution 72/250 met in 2018 and 2019 but ultimately failed to adopt a substantive report (see A/74/77). The Group established pursuant to resolution 77/250 commenced its work in 2023 and will report to the Assembly at its seventy-ninth session. By its resolution 78/238, the Assembly decided to establish an open-ended working group under this item, which will meet between 2024 and 2028.

60. By its resolution 76/231, the General Assembly established the open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, which convened in 2022 and 2023. The working group was not able to adopt a report; however, the views of Member States were summarized in a working paper submitted by the Chair (A/AC.294/2023/WP.22). By its resolution

[16] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, art. IV; and Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and under Water, art. I (1) (a).

78/20, the Assembly decided to establish a new open-ended working group under this item, which will meet in 2025 and 2026.

F. Electromagnetic technologies

61. A variety of weapon technologies exist or are under development that use electromagnetic energy to achieve their primary effect or as a means of propelling a projectile. These weapons can be divided into three general categories: (a) electronic warfare capabilities, which deny, impede or destroy an adversary's ability to access the electromagnetic spectrum; (b) directed-energy weapons, which use electromagnetic energy to cause damage or destruction; and (c) electromagnetically propelled weapons, which use electromagnetic energy to accelerate a solid projectile to a high velocity.

62. Modern military systems frequently rely on sensors, guidance systems and communications that use electromagnetic signals. Electronic warfare systems can be used to attack electromagnetically dependent military assets or safeguard one's own assets. One recent development is the use of electronic warfare systems to disrupt the connection between uncrewed aerial vehicles and their ground stations, which is counteracted by the greater integration of autonomy into those systems. Several States are developing ground-based electronic warfare capabilities to disrupt space-based services. Such capabilities have already been used to disrupt space-based services, including broadcast media and position, navigation and timing. The use of electronic warfare systems, particularly in peacetime, has the potential for the large-scale disruption or disabling of digital connectivity, for example, by jamming Internet satellites and their ground stations.

63. Directed-energy weapons include lasers, high-power microwaves, millimetre waves and particle beams. States have successfully tested terrestrial-based lasers against aerial targets and are developing such systems for use against uncrewed aerial vehicles, rockets, missiles and incoming munitions. One perceived advantage of such systems is their low "cost per shot". Terrestrial-based lasers have also reportedly been used by States to blind, dazzle or potentially destroy the optical sensors of surveillance satellites in low Earth orbit. Research is ongoing regarding very small fibre lasers in arrays, free-electron lasers as directed-energy weapons, and electromagnetic pulses as anti-satellite weapons.

64. Electromagnetically propelled weapons, such as rail or coil guns, could be capable of launching projectiles to greater distances and at greater speeds than chemical propellants. While prototypes have been test fired, technical barriers remain, including the requirement for a large power supply and sufficiently robust components. Such weapons are primarily considered for anti-access/area denial and naval defence roles.

Relevant intergovernmental processes, bodies and instruments

65. Electronic warfare capabilities and directed-energy weapons were discussed by the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space (see A/74/77). The current views of Member States can be found in recent reports of the Secretary-General on the disarmament aspects of outer space, including documents A/76/77 and A/77/80. The open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours discussed issues related to electronic warfare in the context of its mandate, as reflected in the Chair's summary (A/AC.294/2023/WP.22).

G. Materials technologies

66. Advances in materials sciences are playing a key role in enabling innovation across multiple domains relevant to peace and security. For example, novel materials have enabled significant progress in miniaturization, weight reduction, energy efficiency, enhanced protection and physical resistance, and increased stealth capabilities. These properties have been key enabling factors in the development of modern conventional platforms, as well as weapons systems and their parts and components.

67. Additive manufacturing continues to revolutionize manufacturing processes by enabling the decentralized production of an increasing number of parts and components, thereby creating new challenges for the governance and monitoring of supply chains and for export controls. The improvements in both industrial- and commercial-grade printers, the ability to print an increasing number of materials, even with the same device, and the wealth of open-source knowledge have further lowered the barriers for State and non-State actors to build complex components for a wide range of applications in conventional and unconventional weapon systems. In recent years, the cross-regional proliferation and increased durability of automatic small arms produced through additive manufacturing has been of concern. Another recent trend is the use of additive manufacturing to produce ammunition, including small-calibre ammunition; although currently still less effective than conventionally manufactured ammunition, this raises further challenges to small arms and ammunition controls. Additive manufacturing has also increased the significance of intangible transfers of technology and software-based designs in the context of arms control.

68. Developments in nanotechnology have made it easier to produce, transport and deliver chemical and biological agents, potentially hindering non-proliferation efforts. The development of sensors employing nanotechnology is ongoing. Such sensors could be used to detect very small amounts of gases and vapours. These developments could have benefits for disarmament verification efforts. Risks of nanotechnology include the toxic and environmentally hazardous nature of some nanoparticles.[17] Nanotechnology could also facilitate developments in computing technology and can facilitate advanced communications for military operations.

69. Modular weapons are composed of multiple components that can be reconfigured. Such modularity presents particular challenges to the requirement in the International Tracing Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons that a unique marking be included on an essential or structural component of a weapon. In addition, the use of polymer plastics in weapons manufacture has raised concerns, given that markings on such material are more vulnerable to erasure and alteration than on more traditional materials, such as steel.

Relevant intergovernmental processes, bodies and instruments

70. The Security Council, in its resolution 2325 (2016), requested the Committee established pursuant to resolution 1540 (2004) to take note in its work, where relevant, of the continually evolving nature of the risks of proliferation, including the use by non-State actors of rapid advances in science, technology and international commerce for proliferation purposes, in the context of the implementation of resolution 1540 (2004). The Council also encouraged States, as appropriate, to control

[17] UNIDIR, “Enabling technologies and international security: a compendium – 2023 edition”, 6 March 2024, pp. 13–15.

access to intangible transfers of technology and to information that could be used for weapons of mass destruction and their means of delivery.

71. The General Assembly encouraged States to take into account recent developments in small arms and light weapons manufacturing, technology and design, in particular polymer and modular weapons (see Assembly resolution 78/46). In June 2024, the fourth United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects decided to establish an open-ended technical expert group, convening within the week of the Biennial Meetings of States in 2026 and 2028, to develop recommendations by consensus to ensure the implementation of the International Tracing Instrument and the Programme of Action in the light of recent developments in small arms and light weapons manufacturing, technology and design, in particular polymer and modular weapons, and firearms produced using 3D printing. The group shall consider both challenges and opportunities posed by technology developments. Furthermore, States agreed to facilitate the transfer of technology for marking, record-keeping and tracing of small arms and light weapons, to exchange practices to address the illicit manufacture using additive manufacture technologies, and to engage where appropriate with the additive manufacture industry (see A/CONF.192/2024/RC/3).

III. Convergence of technologies

72. The convergence of science and technology involves the interdisciplinary interaction of a particular technological field with both emerging and established technologies. Such convergence presents both opportunities and challenges in the context of international peace and security. Interdisciplinary interactions often lead to innovation and breakthroughs in science. On the one hand, the swift progress in science and technology can foster human development and act as a catalyst for the implementation of the 2030 Agenda for Sustainable Development. On the other hand, the interplay of these technologies can generate unexpected outcomes for international peace and security.

73. Data are the building blocks for technological development and underpin the increasing interactions among several technology areas. The present section provides an overview of the areas of concern often raised in multilateral discussions.

Artificial intelligence and autonomy

74. Artificial intelligence is not a prerequisite for the functioning of autonomous weapons systems. However, when incorporated, it could further enable autonomy.

75. Some of the potential uses of artificial intelligence in the context of autonomous weapon systems include: (a) near-real-time processing of data from various sensors (from ground-based radars to satellites) and electronic signals for target recognition, identification and classification; (b) autonomous navigation in and adaptation to diverse terrains regarding when to fire a weapon and the timing of detonation; (c) real-time threat analysis and selection of course of action or providing possible actions to a human operator to do the selection; (d) learning from past missions and encounters to improve performance over time; and (e) the use of natural language processing and computer vision to enable human-machine interaction.

76. An area of concern for both the use of artificial intelligence in the military domain and autonomy has been the notion of "human control"[18] over the use of force. Many States and non-governmental experts have questioned the acceptable levels of autonomy in critical functions of weapon systems, including target selection and application of force to targets.

77. Within the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems established under the auspices of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, many States have noted that weapon systems operating entirely without "human control" may not be legally or ethically acceptable. Disagreement remains on the required degree of "human control" throughout various stages of the system's "life cycle".[19] There are also differing views on whether "human control" is necessary for compliance with international humanitarian law.

ICTs, artificial intelligence and quantum technology

78. Artificial intelligence-enabled capabilities can provide both risks and opportunities for ICT security.

79. States and private companies increasingly use artificial intelligence to detect potential threats in their ICT networks. For instance, artificial intelligence-enabled systems can automatically detect and block phishing attempts, malware or other malicious activities based on analysis of unusual patterns and anomalies in the network traffic.

80. At the same time, artificial intelligence can also pose ICT-related risks. Artificial intelligence applications, such as large language models, can be repurposed for use by attackers to generate malicious codes, identify system-level vulnerabilities, spread misinformation or break existing encryption methods. While these risks are not unique to large language models or generative artificial intelligence, the risks may be enhanced by them.[20] Artificial intelligence can create "deepfakes", which are realistic but entirely fictitious videos, including of public figures, spreading false information and influencing public opinion. Moreover, cybercriminals can create deepfakes that impersonate the voices of loved ones.[21]

81. Artificial intelligence models could be the subject of malicious ICT activity whereby perpetrators leverage artificial intelligence models to gain access to source codes or data sets or to deliberately inject false or misleading data into training data sets. The latter phenomenon, known as data poisoning, would undermine the safety and security of artificial intelligence systems.

82. Quantum technologies coupled with other technology applications such as ICTs and artificial intelligence can provide both opportunities for and challenges to peace and security. It is expected that quantum key distribution technology will enable secure communications between parties. Quantum key distribution could also provide better encryption and decryption of data, which is essential for the security of digital tools. Quantum technologies are also expected to improve ICT security protocols

[18] At present, there is no agreed terminology among States when referring to human control. Other terms used include meaningful human control, human intervention, human oversight, appropriate human judgment, human agency and human on/in/out of the loop.

[19] The life cycle of artificial intelligence refers to several stages, including but not limited to pre-design, design, development, deployment, use and decommissioning.

[20] Ioana Puscas, *AI and International Security: Understanding the Risks and Paving the Path for Confidence-building Measures* (Geneva, UNIDIR, 2023).

[21] Emily Flitter and Stacy Cowley, "Voice deepfakes are coming for your bank balance", *The New York Times*, 30 August 2023.

based on quantum principles. However, with advanced computing power, quantum computers have the potential to break widely used encryption methods, compromising existing cryptographic systems. This could unearth new vulnerabilities, including for critical infrastructure that provides essential services to the public. The integration of quantum technologies into ICTs is likely to pose additional challenges for countries with limited capacity, thus necessitating tailored capacity-building in this area, for instance by addressing issues of global access to quantum technology and enabling a quantum-literate workforce globally.

83. The open-ended working group on security of and in the use of information and communications technologies 2021–2025 provides an opportunity for Member States to share views on existing and potential threats. In this framework, many Member States have highlighted the risks and opportunities posed by artificial intelligence and quantum technologies, among other technologies, in connection with ICTs.

Artificial intelligence and the life sciences

84. As stated in the Secretary-General's policy brief on A New Agenda for Peace, multiple technologies in the life sciences are advancing and converging to generate considerable potential benefits for society at large. The convergence of the life sciences with artificial intelligence applications enables large amounts of data to be collected and analysed for patterns that can address public health challenges more effectively.

85. However, such advances could also reduce the cost and technical barriers to the development of biological weapons. Artificial intelligence applications could be used to design, synthesize and disseminate harmful biological agents or to develop delivery systems, creating new and advanced biological weapons. Other cascading impacts from the convergence of artificial intelligence and biology could include engineered pandemics or other unforeseen events.

86. The integration of generative artificial intelligence into protein design and drug discovery is rapidly transforming approaches to health challenges by helping scientists and developers to speed up the process of predicting how new proteins and small molecules work, along with how they interact with other molecules. This accuracy could revolutionize pharmaceutical research and development but also poses significant dual-use concerns.[22] Advancements in the design of proteins and other molecules have the potential to enhance the virulence or resistance of pathogens, raising concerns about their possible use as biological weapons. This potential misuse underscores the urgent need for international dialogue and cooperation to ensure that these technologies are applied responsibly.

87. The rise of automated or semi-automated chemical synthesis, whereby robotic platforms, fuelled by generative artificial intelligence, either assist or fully perform synthesis operations, promises to streamline the production of chemicals, potentially reducing costs, lead time and complexity. Fully automated systems may even lower the barriers to use, allowing non-specialists to perform complex chemical transformations. While this can drive innovation, it also raises the possibility of covert production of dangerous substances. This presents significant challenges to international peace and security, as it could facilitate the proliferation of chemical agents and complicate the oversight and monitoring of dangerous substances.

[22] See https://www.nature.com/articles/d41586-024-00699-0, https://www.technologyreview.com/2023/02/15/1067904/ai-automation-drug-development/, https://communities.springernature.com/posts/cavitomix-drug-solver-a-gpu-accelerated-tool-for-drug-repurposing-and-off-target-analysis-using-cavity-property-point-clouds-on-nvidia-dgx-a71725f0-77f6-46e5-8a3d-9c6d19aae6b6 and https://www.nvidia.com/en-us/clara/bionemo/.

Life sciences and ICTs

88. The convergence of biology with ICTs[23] has profoundly affected the nature of life science research, creating new opportunities for collaboration and accelerated research, for instance through increased access to data sets. Such convergence could, however, also generate significant risks, including the exploitation of network vulnerabilities in the health sector, including medical centres, and biological laboratories, as well as the supply chain.[24] Furthermore, there is concern over potential manipulation of research data and unauthorized access, leading to the release of private health information. This could undermine public trust in health institutions, complicate efforts to counter global pandemics, and heighten tensions between States over the implementation of norms in ICT security.

Nuclear weapons, ICTs and artificial intelligence

89. Nuclear weapons were first developed when computer capabilities were in their infancy.[25] Accordingly, little attention was given to the potential implications of artificial intelligence and ICT security, both of which now pose distinct potential challenges to nuclear weapons and their associated command-and-control and early warning systems.

90. Malicious ICT activities during peacetime could increase tensions and heighten the likelihood of conventional armed conflicts between nuclear-armed States, thereby increasing the potential for nuclear escalation (see A/76/182). During armed conflict, malicious ICT activity targeting nuclear weapons systems or dual-use systems, such as early warning systems, may lead to misperception and miscalculation, potentially resulting in the inadvertent use of a nuclear weapon.

91. Experts have identified activities, such as hacking, spoofing, interference and other malicious actions aimed at exploiting potential ICT vulnerabilities in nuclear weapons systems. These vulnerabilities include:[26] (a) communications between command and control systems; (b) communications from command stations to missile platforms (e.g. submarines) and missiles; (c) telemetry data from missiles to ground- and space-based command and control assets; (d) analytical centres for gathering and interpreting data; (e) digital technologies in transport; (f) digital technologies use in laboratories and assembly facilities; (g) real-time targeting information from space-based systems, including position, navigation and timing data; (h) positioning data for launch platforms; (i) real-time targeting information from ground stations; and (j) autonomous or artificial intelligence-enabled systems integrated into command, control or communications.

92. States parties to the Treaty on the Non-Proliferation of Nuclear Weapons, individually and in groups, have expressed concern about the nexus between these technologies and nuclear weapons, including in various working papers submitted throughout the review cycle of the Treaty.[27]

93. The integration of artificial intelligence into nuclear weapons and potential ICT vulnerabilities in nuclear command, control and communication systems could

[23] See https://documents.unoda.org/wp-content/uploads/2021/04/07_31_Pauwels_Slides_MX2.pdf.

[24] Lauren C. Richardson and others, “Cyberbiosecurity: a call for cooperation in a new threat landscape”, *Frontiers in Bioengineering and Biotechnology*, vol. 7 (June 2019).

[25] See https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

[26] UNIDIR, *Understanding Nuclear Weapon Risks*, John Borrie, Tim Caughley and Wilfred Wan, eds. (Geneva, 2017).

[27] See, for example, NPT/CONF.2020/WP.6, NPT/CONF.2020/WP.9/Rev.1, NPT/CONF.2020/WP.70, NPT/CONF.2026/PC.I/WP.24 and NPT/CONF.2026/PC.I/WP.30.

potentially undermine international stability and have an impact on security concepts, such as mutual deterrence (ibid.). Actors with malicious intent could exploit ICT vulnerabilities to launch non-kinetic attacks, for example spoofing or hacking early warning systems, to cause false alarms or disruptions in network security that could escalate to unintended nuclear confrontations. Artificial intelligence could increase the sophistication of those attacks. During armed conflict, concerns about interference with nuclear weapons systems could create destabilizing conditions under which States feel compelled to use nuclear weapons first, leading to rapid and uncontrolled escalation.

94. The integration of artificial intelligence into nuclear weapons systems, such as autonomous control or pre-delegation to launch nuclear weapons, could result in catastrophic consequences. Technical challenges to artificial intelligence safety such as data poisoning and potentially unpredictable decision-making ("black box")[28] raise particular concerns about the possible credibility of information that is critical to nuclear decision-making and increase prospects for the inadvertent use of nuclear weapons. The use of artificial intelligence in nuclear command, control and communications could lead to compressed time frames for decision-making, whereby the speed of artificial intelligence-enabled actions can outpace human capacity, resulting in miscalculation and escalation during crises. To avoid such potential outcomes, three nuclear-weapon States, in their working paper to the tenth Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons (NPT/CONF.2020/WP.70), stressed their commitment to maintaining "human control and involvement for all actions critical to informing and executing sovereign decisions concerning nuclear weapons employment".

IV. Conclusions and recommendations

95. United Nations entities will continue to support and facilitate existing and potential new processes to address emerging challenges before they can pose a danger to peace and security, human rights, humanitarian norms and principles, or other purposes and objectives of the Organization. It is recommended that Member States identify multilateral forums to discuss synergies across the technologies considered in the present report.

96. The Disarmament Commission has agreed to consider an agenda item entitled "Recommendations on common understandings related to emerging technologies in the context of international security" during its 2024–2026 triennial cycle. This is an important opportunity for Member States to consider cross-cutting considerations applicable to all emerging technologies, as well as to consider those emerging technologies that have implications for international security but are not currently discussed in United Nations processes.

97. It is recommended that United Nations bodies and entities continue to encourage multi-stakeholder, geographically equitable and gender-balanced engagement, including by academia, industry and other private sector actors, through formal and informal platforms.

98. Member States are encouraged to continue to seek ways of integrating reviews of developments in science and technology in their work within all relevant United Nations disarmament bodies, including through processes for reviewing the operation

[28] In computing, a "black box" is a system for which the inputs and the outputs are known but not the process by which the system turns the former into the latter. It is when the internal working and the decision-making processes of an artificial intelligence system are opaque and not explainable or understandable to humans. See https://unidir.org/files/2020-09/BlackBoxUnlocked.pdf.

of disarmament treaties. This could entail the development of science and technology review mechanisms, when relevant, to inform intergovernmental discussions. The review mechanisms should ensure the identification and examination of new or emerging technologies that perpetuate or amplify social biases, including gender bias, and their impact on the application of international law.

99. The Summit of the Future, to be convened on 22 and 23 September 2024, represents an important opportunity to take visionary and concrete action in relation to emerging technologies and their impact on peace and security. I urge Member States to act on the recommendations in my policy brief on A New Agenda for Peace in this regard.

100. It is recommended that the General Assembly continue to request reports containing updates to the information in the present report on an annual basis, as a contribution to maintaining awareness of developments in science and technology and their potential impact on international security and disarmament efforts.