United Nations A/77/188

General Assembly

Distr.: General
18 July 2022

Original: English

Seventy-seventh session
Item 99 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 76/24. It covers artificial intelligence and autonomous systems, digital technologies, biology and chemistry, space and aerospace technologies, electromagnetic technologies and materials technologies. In addition, implications of new technologies on existing legal frameworks related to the use of force are addressed in the report.

* A/77/150.

22-11266 (E) 290722

Contents

I. Introduction

1. In paragraph 4 of its resolution 76/24 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-seventh 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. It is important that efforts to govern new weapon technologies or weapon applications of new and emerging technologies do not hamper the economic or technological growth of any State.

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 understand and manage the risks. As the Secretary-General laid out in his 2018 disarmament agenda *Securing Our Common Future: An Agenda for Disarmament*, the international community must remain vigilant in understanding new and emerging weapon technologies that could imperil the security of future generations and could pose challenges to existing legal, humanitarian and ethical norms, non-proliferation, international stability, and peace and security.

4. 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.

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

A. Artificial intelligence and autonomous systems

5. There is no universally agreed definition of artificial intelligence, but broadly speaking, it relates to machines with the ability to learn, solve problems, make predictions, take decisions and perform tasks that are considered to require human intelligence. Contemporary artificial intelligence comprises a number of subfields such as machine learning, and applications and uses, such as analytics, and visual and language processing. While manually coded programmes generally contain specific instructions on how to complete a task, machine learning is focused on ways in which computers can learn without being explicitly programmed with instructions for generating outputs. Machine learning is highly dependent on the quality and volume of input and training data and on decisions made during design, development and testing. Both data and design decisions can cause unintended vulnerabilities and biases.

6. The majority of artificial intelligence research and development occurs in the civilian sphere. Recent advances in machine learning have primarily been fuelled by faster processors and the availability of ever larger data sets. A number of qualities make artificial intelligence appealing, including the potential for greater efficiency and automation as well as substantially enhanced analytical capabilities. Current artificial intelligence applications are narrow in focus; thus, general artificial intelligence abilities, those that can apply knowledge and skills from one domain to another, are unlikely to be available in the near future.

7. Autonomy refers to a system's ability to execute tasks or functions of varying levels of complexity without human input or control. While there are other mediating factors, including a debate around when the human action occurs, autonomous systems either (a) require human input at some point during the execution of the task (human-in-the-loop or semi-autonomous); (b) execute tasks independently but under the supervision of a human who can intervene (human-on-the-loop); or (c) operate independently of human involvement or supervision (human-out-of-the-loop). The elements of an autonomous system can be integrated into one machine or be physically distributed between geographically dispersed sites.

Military applications and implications

8. Military applications are broad, and many include non-weapon functions, such as operational support and logistics. Some States already test or field a variety of artificial intelligence-enabled systems, including uncrewed systems in the air, land and maritime domains capable of autonomous navigation; coordinated mobility and swarming systems; systems that sort and analyse intelligence data; defensive and offensive information and communications technology systems; and simulation and training applications.

9. Autonomous weapon systems are generally understood to employ autonomy in critical functions during an attack, including target selection and the firing of a weapon. Systems that employ autonomy only in other functions, such as navigation, would not generally be regarded as autonomous weapons. The definition of an autonomous weapon system is the subject of continuing international deliberations (see CCW/GGE.1/2019/3). However, there are weapon systems already deployed that, once activated, are capable of selecting and engaging targets autonomously, without further human intervention, albeit in a limited range of environments. Examples include close-in weapon systems deployed on naval ships and guided munitions that select a specific target after being fired on the basis of general or preselected criteria.

10. In commonly cited potential applications of autonomy in weapons, the autonomous functions would carry out tasks that are tedious or repetitive or require more endurance, speed, reliability or precision than a human operator. These attributes can make such systems attractive to armed forces as well as to non-State armed groups, although such groups may accept substantially lower thresholds for accuracy and reliability. States have expressed various concerns about the potential challenges posed by autonomous weapon systems, including for ensuring respect for international humanitarian law and other bodies of international law, the maintenance of international peace and security, and ethical considerations.

Relevant intergovernmental processes, bodies and instruments

11. The sixth Review Conference 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 decided to continue the work of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, with the mandate to consider proposals and elaborate, by consensus, possible measures, including taking into account the example of existing protocols within the Convention, 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 of Governmental Experts related to emerging technologies in the area of lethal autonomous weapon systems, and bringing in expertise on legal, military, and technological aspects.

B. Digital technologies

12. “Digital technologies” is an umbrella term for a range of technologies that process information in a binary numerical format. They permeate every facet of contemporary life and drive innovation in all sectors of society. The increasing reliance on ever more advanced, complex and interconnected digital technologies has led to new vulnerabilities as well as the development of harmful information and communications technology (ICT) instruments. These vulnerabilities and instruments can be utilized for a range of purposes, including for malicious activities that can pose a threat to international security, stability, and economic and social development, as well as the safety and well-being of individuals. Moreover, a number of States are developing ICT capabilities for military purposes. The present section is focused on developments in the field of digital technologies relevant to international peace and security, namely ICTs, including their convergence with artificial intelligence; the dark web; and quantum technologies.

Information and communications technologies

13. ICTs, which can be considered a subcategory of digital technologies, comprise a diverse set of tools and resources used to transmit, store, create, share or exchange information, including through the use of the Internet. Global reliance on ICTs continues to grow through new developments in, inter alia, network technology, data science, cloud computing and the Internet of things. As the composition of ICT software and hardware is generally becoming more complex and the demand for interoperability and integration of platforms and devices rises, the risk of security vulnerabilities and the potential exploitation of ICT products and systems is also growing. There is also a risk that vulnerabilities present in weapons systems may be exploited. States have expressed concern over developments in the global ICT environment, including a dramatic increase in incidents involving the hostile or malicious use of ICTs by State and non-State actors. Incidents of concern include those affecting critical infrastructure and associated information systems of States. The harmful use of ICTs could increase the risk of misperception, miscalculation and unintended escalation between States and may jeopardize international peace and security.

14. Harmful activity can be directed at different types of ICT networks and systems and can be channelled through different layers of the Internet,[1] including its physical infrastructure, network and routing functionalities, and applications and content. It can also affect technologies that rely on several of these elements, such as cloud-based services or networked devices. Various methods are used to target ICT-enabled systems and to exploit vulnerabilities.[2] Malicious software, or malware, is designed to harm or exploit ICT-enabled devices, services or networks, at times through a vulnerability unknown to the product owner or user. Types of malware include viruses, trojans, worms, cryptojacking and botnets. Malware is commonly transmitted through social engineering, whereby a user is lured into activating it under false pretences. The proliferation of ransomware, a form of malware designed to encrypt files on a device, rendering any files and/or the systems that rely on them unusable until the ransom is paid, can be particularly problematic in the context of critical infrastructure. Ransomware is an attractive avenue for malicious actors owing to a

[1] This refers to a simplified version of the Open Systems Interconnection model, in which the Internet is conceived as consisting of seven layers.

[2] See the survey of threats and vulnerabilities in the ICT environment in Camino Kavanagh, “Stemming the exploitation of ICT threats and vulnerabilities: an overview of current trends, enabling dynamics and private sector responses”, United Nations Institute for Disarmament Research, 2019.

perception of high reward and of low risk of apprehension. Harmful activity targeting the network and routing functionalities of the Internet includes the manipulation of routing protocols and distributed denial-of-service attacks, whereby a high volume of traffic is directed at a server, often through the use of malware, with the aim of overloading it. Activity that undermines the integrity of the domain name system and other protocols can also have a severe impact, as can interference with physical ICT infrastructure, such as undersea cables, space systems and networks.

Information and communications technologies and artificial intelligence

15. Artificial intelligence can be used to protect ICT systems from malicious intrusion. Software that employs algorithms may be used to efficiently scan operating software and security systems to identify system- and network-level vulnerabilities. Algorithms that scan and analyse large data sets, including from social media and data breaches, can also improve the effectiveness of social engineering techniques. Moreover, malware with autonomous functions can move laterally, without detection, within networks by learning the normal patterns of business operations and security protocols. In addition, harmful ICT activity, such as distributed denial-of-service attacks, can be automated, which can facilitate a larger number of incidents at quicker speeds.

The dark web

16. The dark web refers to the part of the Internet that is not accessible by traditional search engines and is hidden behind anonymity software. There have been reported misuses of the dark web to facilitate the illicit trade in firearms, ammunition and explosives.[3] Also of concern is the use of the dark web by non-State actors to facilitate the transfer of materials and technologies for the development of weapons of mass destruction. Undisclosed software vulnerabilities in ICT systems are also known to be traded on the dark web.

Quantum technologies

17. The integration of quantum properties, most notably entanglement and superposition, into functions such as computation, sensing and imaging, and cryptography can have a considerable enabling and transformative impact, including for international peace and security. For example, quantum computers allow for exponentially higher computing speeds and an ability to solve problems of higher complexity. Quantum sensing and imaging allow for the capture of objects with a resolution beyond what is possible with classical sensor technologies. Quantum cryptography is a method of encryption that is highly secure, thus proving useful for the protection of critical infrastructure and other vulnerable ICT systems. In addition to those potential benefits, there remains the possibility that the same advances in quantum technologies could pose risks to international peace and security.

Relevant intergovernmental processes, bodies and instruments

18. 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.[4] Since 2004, the Assembly has established six groups of governmental experts to study possible cooperative measures to address existing and potential threats in the ICT environment. Four of these groups have agreed on substantive reports with

[3] See Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web: A Study* (New York, Office for Disarmament Affairs (UNODA) Occasional Papers No. 32, 2018).

[4] 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.

recommendations to address the threats posed by the use of ICTs, including recommendations on norms, rules and principles for the responsible behaviour of States, confidence-building measures capacity-building, and the ways in which international law applies to the use of ICTs (see A/65/201, A/68/98, A/70/174 and A/76/135).

19. The open-ended working group on developments in the field of information and telecommunications in the context of international security established by the General Assembly pursuant to its resolution 73/27 adopted a report by consensus in March 2021 (A/75/816). The General Assembly endorsed the report and its recommendations in decision 75/564. The group of governmental experts on advancing responsible State behaviour in cyberspace in the context of international security, established pursuant to General Assembly resolution 73/266, adopted a consensus report in May 2021 (A/76/135), which included an additional layer of understanding to the findings and recommendations of the previous groups.

20. In 2020, the General Assembly established a new 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 information and communications technologies by States; and consider confidence-building measures and capacity-building.

C. Biology and chemistry

21. 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, combined with advances in chemistry and biology, threaten to undermine legal and normative measures. The coronavirus disease (COVID-19) pandemic has exposed the vulnerability of modern societies to biological agents, which could also have attracted the interest of some State and non-State actors.

22. Multiple technologies in the life sciences are advancing and converging to generate considerable potential benefits for society at large. However, the same technologies also raise significant safety and security issues. Trends in a number of broad areas are facilitating advances. For example, advances in genome editing technologies such as CRISPR/Cas9 enable relatively easier and more precise manipulation of the genetic code of life, as a result of which it is now possible to read, write and, increasingly effectively, edit DNA. The convergence of the life sciences with big data and machine learning enables large amounts of data to be collected and analysed for patterns that can address public health challenges far more quickly than ever before.

23. Research and development in such fields are overwhelmingly undertaken for peaceful purposes. Along with other technologies, these developments could play a significant role in addressing societal challenges as well as strengthening the international legal regime against biological weapons. For example, big data and DNA sequencing could aid investigations of non-compliance with the Biological Weapons Convention as well as facilitating the provision of assistance in the event of a violation. However, several ethical, legal, safety and security concerns exist. They include developments that could feed into new forms of biological weapons, ease access to or production of known biological weapons, or complicate existing means of detecting and responding to disease.

24. For example, improved understanding of immunology could facilitate the development of vaccines and therapeutics. However, the same knowledge could be exploited for hostile purposes in developing new weapons capable of more effectively overwhelming or avoiding recognition by the immune system as well as rendering medical countermeasures such as vaccine stockpiles ineffective. Advances in understanding human genetics and reproductive science could play a role in treating infertility and genetically inherited diseases. Yet such technology has raised ethical and safety concerns that it could be exploited for hostile purposes.

25. With regard to chemical weapons, the remarkable progress made in understanding life processes at the molecular level has resulted in a greater ability to manipulate and interfere with such processes. Capabilities in those areas are expected to continue to grow. Computational tools to design molecules that can target specific cell types and highly active pharmaceutical-based chemicals that act on the central nervous system have led to concerns about the possibility of new types of toxic chemical weapon agents. To this end, in late 2021, States parties to the Chemical Weapons Convention clarified the prohibition of the aerosolized use of chemicals that act on the central nervous system for law enforcement purposes. There is also increased risk from more rudimentary chemical weapons. The growing availability of knowledge of improvised chemical dispersal devices combined with easy access to commercially available toxic chemicals presents new challenges for security and disarmament.

26. The crossover between the domains of biology and chemistry also requires consideration. Chemicals are increasingly being produced using biologically mediated processes, such as microbial fermentation or the use of enzymes as catalysts. In addition, substantial advances have been made in the chemical synthesis of molecules of biological origin. Multidisciplinary research teams continue to expand beyond biology and chemistry to incorporate ideas and approaches from other disciplines, including computing, materials science and nanotechnology. That convergence provides significant social and economic benefits, including through improved defensive countermeasures against chemical and biological warfare agents. However, such new approaches and processes, combined with developments in drug discovery and delivery, could also be exploited in the development of new toxic chemicals to be used as weapons or in the modification of biological agents on a molecular level to affect the course of infection, transmission, and severity of disease.

Relevant intergovernmental processes, bodies and instruments

27. 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 will take place in November and December 2022. The fifth Review Conference of the States Parties to the Chemical Weapons Convention will take place in 2023.

28. Both treaties also have more regular means of reviewing relevant developments in science and technology. The Chemical Weapons Convention established a Scientific Advisory Board. In 2021, the Board convened its thirty-first, thirty-second and thirty-third sessions. In addition, its temporary working group on the analysis of biotoxins held its second and third meetings in the same year. Furthermore, the Organisation for the Prohibition of Chemical Weapons is in the process of establishing the new Centre for Chemistry and Technology that will enable the Organisation to conduct research activities to support and strengthen the verification regime, as well as conducting training courses and other capacity-building activities.

29. While several proposals for a scientific advisory body or mechanism for the Biological Weapons Convention have been made, States parties have not thus far

agreed on such an approach. From 2012 to 2015, a review of developments in the field of science and technology related to the Convention was a standing agenda item. In 2018, States parties established an annual meeting of experts to review developments in the field of science and technology related to the Convention. The importance of the discussions on the convergence between the Biological Weapons Convention and the Chemical Weapons Convention has been recognized, and the discussions now take place in a biennial forum on the topic organized by Switzerland.

30. Pursuant to Security Council resolution 1540 (2004), States are required to establish and strengthen controls to prevent the proliferation of biological and chemical weapons and their means of delivery to non-State actors.

D. Space and aerospace technologies

Missile technologies

31. Developments in emerging technologies are enabling new and expanded functions of missile systems, with implications for international peace and security and efforts to ensure the effective regulation of arms, non-proliferation and respect for humanitarian principles.

Accuracy

32. A growing number of States continue to pursue and refine various technological innovations to increase the accuracy of their ballistic missiles and artillery rockets. Such innovations have included the incorporation of modern avionics into missile systems; flight trajectory tracking, including by ground-based radar, optical sensors, radar imaging, and navigation and positioning satellites; post-boost vehicles that enable a warhead to manoeuvre outside the atmosphere; and the deployment of re-entry vehicles with aerodynamic controls, enabling those weapons to manoeuvre in the atmosphere, including in the terminal phase of flight.

33. Increases in the accuracy of nuclear-capable missiles can enable more States to deploy strategic weapons with smaller nuclear explosive yields, or with conventional warheads. Nuclear weapons with smaller or variable yields can potentially be assigned to an expanded range of roles and military missions, affecting perceptions of “usability”.

34. Increases in the accuracy of missile systems have ostensibly enhanced the perception of the military utility of ballistic missiles as tactical or battlefield weapons, as demonstrated by their proliferation and use in recent armed conflicts, including by State and non-State actors.

35. Increases in the accuracy of large-calibre artillery rockets have resulted in the development of systems that blur distinctions between artillery rockets and ballistic missiles capable of delivering a nuclear weapon. That trend poses a challenge to regimes designed to curb the proliferation of ballistic missiles capable of delivering nuclear weapons.

36. Manoeuvrable warheads can be intended to avoid anti-missile systems. That provides incentives to States to improve and develop capabilities and concepts for missile defence, some of which can exacerbate tensions or even international instability in certain contexts, in the light of different views on the relationship between offensive and defensive weapon systems.

Hypersonic glide vehicles

37. Ballistic missiles typically reach hypersonic speeds[5] during their flight. Some States are developing and deploying vehicles with the ability to glide and manoeuvre at hypersonic speeds over long distances within the atmosphere, sustained by aerodynamic lift. Like a manoeuvrable re-entry vehicle, a hypersonic glide vehicle would be launched from a booster rocket. Thus, 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.

38. Research into hypersonic glide vehicles began decades ago. The first known weapon, possibly nuclear-armed, deployed on hypersonic glide vehicles entered into service in 2019, using an intercontinental-range ballistic missile as a booster. Those developments have led to concerns about new strategic arms competition and may be prompting interest in long-range conventional strike capabilities by a growing number of States.

Powered hypersonic vehicles

39. Most existing types of cruise missiles using traditional jet turbine engines are limited to travelling at subsonic speeds. As a means of developing systems that are more capable of evading air defence and anti-missile systems, a number of States are developing and testing cruise missiles that use new engine types, including scramjets, enabling sustained flight at hypersonic speeds. Scramjet engines are typically accelerated to supersonic speeds by a boost vehicle before they can sustain powered flight. In recent years, a number of States have tested hypersonic cruise missiles powered by scramjet engines, and a variety of such weapon systems are being designed for launch by ground-, sea- and aircraft-based boosters and armed with conventional or possibly nuclear warheads.

Anti-missile and terrestrial anti-satellite systems

40. There has been rapid growth in the capability and proliferation of anti-missile systems in recent decades, certain developments of which may have implications for international peace, security and stability as well as for disarmament efforts.

41. Surface-to-air systems that intercept their target within the lower atmosphere are increasingly common and have been extensively used in some armed conflicts and other situations, designed to counter shorter-range ballistic missiles and rockets in the terminal phase of flight. Generally, such systems have not raised concerns about stability, although their widespread deployment may prompt rivals to develop countermeasures.

42. The use of directed energy anti-missile systems, including lasers mounted on aircraft, has been explored, although no such system has been deployed. Proponents of the concept argue that such systems could be used for defence against missiles in the boost phase. In many situations, that would entail the forward deployment of such capabilities near launch sites, possibly leading to concerns about stability.

43. Some anti-missile systems are designed to strike missiles outside of the atmosphere in the mid-course phase of flight. Such systems can use kinetic impactors or explosives. The more capable of those systems have a de facto ability to strike satellites in low Earth orbit. Analysts consider that striking a satellite is easier than striking a ballistic missile, given that satellites travel in predictable paths that can be accurately measured far in advance and generally lack any means of evading threats.

[5] Generally understood as greater than five times the speed of sound.

Serious concerns have been expressed about strategic anti-missile systems designed to counter strategic nuclear weapons, given their ability to strike satellites and the impact of such systems on security concepts based on mutual deterrence.

44. Terrestrial missiles have reportedly been specifically developed to strike satellites in low Earth orbit. The test launch of a direct-ascent missile capable of striking a satellite at the altitude of geostationary orbit has also been reported. To reach such altitudes, a booster would likely require the capability of a medium-lift space-launch vehicle, possibly blurring the lines between space launch vehicles and offensive weapons.

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/63/178). Although the issue of missiles remains on the agenda of the First Committee, there has been no resolution on the topic since 2008 (see General Assembly resolution 63/55).

46. There are two intergovernmental regimes 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 143 States subscribe to the Code.

47. It has been reported that the Russian Federation and the United States of America have discussed hypersonic glide vehicles in bilateral strategic arms reduction talks.

48. 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 open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours. On 18 April 2022, the United States of America announced a national commitment not to conduct destructive, direct-ascent anti-satellite missile testing. Canada announced a similar commitment on 9 May 2022.

Space-based technologies

49. While military and security interests drove early efforts to access and use outer space, the use of outer space today serves a broad range of civil, commercial, economic and military activities. Military forces are increasingly dependent on space-based technologies for fundamental tasks, such as early warning systems, navigation, surveillance, targeting and communication. Space systems, including satellites, are particularly vulnerable to various counter-space capabilities, including the harmful use of ICTs, electromagnetic interference, laser dazzling, spoofing and jamming, and terrestrially launched anti-satellite weapons. The present section is focused on recent developments in space-based technologies with possible anti-satellite applications.

On-orbit servicing and active debris removal

50. Robotic on-orbit servicing capabilities are being developed by national civilian and military entities and commercial companies. Such capabilities rely on a number of component functions, including manoeuvring, close approach, rendezvous, docking and grappling. Certain operations require some of those functions to be performed

autonomously. Applications for such capabilities include satellite refuelling, repair and transportation. Systems capable of such activity in both low Earth orbit and geostationary orbit are being actively developed and brought into operation.

51. The related concept of active debris removal refers to the use of a third-party spacecraft to dispose of space debris. Various State and commercial entities are developing and testing such systems through a variety of technological techniques. Most involve rendezvousing with a target, capturing it and modifying its trajectory so that it will burn up in the atmosphere. Strategies being explored include the use of small satellites equipped with robotic arms, nets, harpoons and adhesives. There have also been academic studies on the feasibility of using space-based lasers to destroy relatively small-scale space debris. No such systems have been put in regular service, although certain concepts have been tested in space.

52. While automated rendezvous and proximity operations in space have been carried out for decades, on-orbit servicing differs in the sense that it involves interactions between two space objects that were not both specifically designed to cooperate with each other. There is concern that satellites capable of performing rendezvous and proximity operations could be used for unwanted, risky, disruptive or hostile acts or that it would be impossible to interpret their purpose directly from their behaviour, particularly given their ability to approach a satellite without its cooperation and in the absence of norms for the responsible use of such systems.

Space-based lasers

53. Space-based lasers with power as low as 10 watts can potentially dazzle or temporarily blind sensors. Some experts believe 40-watt lasers can damage certain sensitive components. The first laser-based communication system was deployed in November 2016. Such means are less susceptible to conventional jamming techniques than radio communication. The further development of such systems could lead to increasing deployment of higher-powered space-based lasers. Research is also under way into the use of space-based lasers for deflecting asteroids or other objects posing a risk to Earth.

Relevant intergovernmental processes, bodies and instruments

54. 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.

55. The prevention of an arms race in outer space has been on the agenda of the Conference on Disarmament since 1985 and has been one of the core issues on its agenda for more than two decades.

56. The Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities agreed upon a consensus report in 2013 (A/68/189). Since 2018, the Disarmament Commission has considered the item: “In accordance with the recommendations contained in the report of the Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities (A/68/189), preparation of recommendations to promote the practical implementation of transparency and confidence-building measures in outer space activities with the goal of preventing an arms race in outer space”. 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. The Committee subsequently re-established the

Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee with a five-year plan, commencing in 2021.

57. The Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, established pursuant to General Assembly resolution 72/250, discussed a number of emerging issues, including possible measures related to rendezvous and proximity operations as well as active debris removal (see A/74/77).

58. By its resolution 76/231, the General Assembly established an open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours with a mandate to, inter alia, make recommendations on possible norms, rules and principles of responsible behaviours relating to threats by States to space systems, including, as appropriate, how they would contribute to the negotiation of legally binding instruments, including on the prevention of an arms race in outer space.

E. Electromagnetic technologies

59. 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, such as rail or coil guns, that use electromagnetic energy to accelerate a solid projectile to a high velocity.

60. Modern military systems frequently rely on sensors, guidance systems and communications that use electromagnetic signals. Electronic warfare systems exploit that reliance through jamming, disrupting or spoofing those signals. The term also encompasses systems for countering such attacks. Electronic warfare systems can be human-portable, fixed, or mounted on ground vehicles, crewed and uncrewed aircraft, ships and missiles. They could hypothetically be deployed under the sea or in outer space. As such, electronic warfare systems have the potential for the large-scale disruption or disabling of digital connectivity, for example by jamming Internet and positioning, navigation and timing satellites and their ground stations. The use of such systems can fall within a grey area that some States may regard as being below the threshold of the use of force or armed attack. Nonetheless, the potential use of such capabilities to target critical military infrastructure, such as early warning satellites, has raised concerns in recent years.

61. Directed-energy weapons include lasers, high-power microwaves, millimetre waves and particle beams. Of those, terrestrial-based and naval high-energy lasers may have the most immediate potential for destructive and disruptive applications. Laser weapons and high-power microwaves are of particular interest for air and missile defence, especially to counter uncrewed aerial vehicles, given their precision, speed and low cost per "shot". Terrestrial-based lasers have also reportedly been used by States to blind or dazzle the optical sensors of surveillance satellites. Research is ongoing regarding very small fibre lasers in arrays, free-electron lasers as directed-energy weapons, and electromagnetic pulses as anti-satellite weapons.

62. Electromagnetically propelled weapons, such as rail or coil guns, could have ranges up to 200 km and could be capable of launching projectiles to greater speeds than chemical propellants. At short ranges, the projectiles could be capable of destroying targets with kinetic energy alone. While advances have aided the development of prototypes, 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. The test-firing of railguns has taken place, and such weapons are expected to be deployed before the end of the present decade.

Relevant intergovernmental processes, bodies and instruments

63. 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 outer space, including document A/76/77 and the report to be issued pursuant to General Assembly resolution 76/230. The open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, established pursuant to General Assembly resolution 76/231, is expected to discuss issues related to electronic warfare in the context of its mandate.

F. Materials technologies

64. The present section addresses developments in both manufacturing techniques and new types of materials.

65. Additive manufacturing has brought novel changes to production. It has also lowered the technological threshold for State and non-State actors to build complex components, including production equipment for fissile materials and chemical or biological weapons. While technical limitations remain, the potential for the use of additive manufacturing for proliferation purposes increases every year. That is especially true when combined with enabling technologies such as artificial intelligence, which can, inter alia, reduce the risk of error, facilitate automated production and, through simulated prototyping, make feasible the printing of previously “unprintable” components.

66. Additive manufacturing is already used by some States to produce nuclear-weapon-related items, such as high-explosive lenses in nuclear warheads. Furthermore, the additive manufacturing supply chain is becoming increasingly difficult for governments to monitor. Additive manufacturing decentralizes production, potentially obviating export controls. It has also increased the significance of intangible transfers of technology and software-based designs in the context of arms control.

67. Developments in nanotechnology have made it easier to produce and transport chemical and biological agents, potentially hindering non-proliferation efforts. Nanotechnology can also enhance the means of delivery for lethal biological and chemical agents by enabling new and improved processes of encapsulation and aerosolization. When coupled with synthetic biology and chemistry, the technology could also aid in the development of novel agents with enhanced lethality and resilience. The development of sensors employing nanotechnology is ongoing. Such sensors could be used to detect very small amounts of gases and vapours; those developments could have benefits for disarmament verification efforts.

68. Trends in small arms and light weapons manufacture and design have continued to raise concerns regarding the durability of weapons marking and, by extension, the ability of States to keep accurate records and undertake effective tracing. 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

69. The Security Council, through its resolution 2325 (2016), expressed its commitment to consider 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 to control access to intangible technology transfers and to information that could be used for developing weapons of mass destruction and their means of delivery.

70. At the seventh Biennial Meeting of States to Consider 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, States undertook, inter alia, to continue to exchange views on recent developments in small arms and light weapons manufacturing, technology and design, in particular polymer and modular weapons, and on ways of addressing them, and to consider the proposal of an open-ended technical expert group at the eighth Biennial Meeting of States on Small Arms (see A/CONF.192/BMS/2021/1, annex). In parallel, 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, and called upon the Secretariat to develop a good practice document on marking practices for modular and polymer weapons taking into account the views of all Member States and the role of manufacturers (see Assembly resolution 76/232).

III. Implications of new technologies for existing legal frameworks related to the use of force

71. In his 2020 report on this item (A/75/221), the Secretary-General observed that "new weapons technologies could also strain existing legal frameworks, including by facilitating the use of force through non-traditional means, such as electromagnetic jamming, and also in ways that are difficult to understand in the light of traditional thresholds for exercising the right of self-defence". Various intergovernmental processes have been aimed at increasing common understanding of what constitutes a use of force or an armed attack when it involves the use of certain emerging weapon technologies or acts carried out in new domains such as cyberspace or outer space. The present section provides a summary of past and continuing work within the United Nations system, including the various views and positions that have been expressed by States on this matter in connection with specific emerging weapon technologies and new domains.

72. Various types of emerging weapon technologies and the emergence of possible new domains in which armed conflict may occur has posed challenges for States to reach a common understanding of the application of international law. This lack of a common understanding can erode trust and confidence in the development and use of dual-use technologies such as ICTs (see A/68/98, paras. 5–10) or satellites designed for rendezvous and proximity operations, which can be used for civil and other legitimate purposes or for malicious or hostile purposes (see A/76/77, para 14 (d)). It also can result in unintended escalation from the use of weapon technologies that have disruptive or reversibly harmful effects that fall below what a State could consider the threshold for the use of force or for the exercise of its right to self-defence, but that might nonetheless be interpreted as a threat or hostile act (see A/76/77, para 16).

73. Many States have cited the jurisprudence of the International Court of Justice in their statements regarding criteria that should be applied in determining whether acts committed using various emerging weapon technologies or in new domains constitute an armed attack. In particular, States referred to the distinction made by the Court between the use of force, within the meaning of Article 2 (4) of the Charter, and an armed attack, within the meaning of Article 51 thereof. The Court distinguished the most grave form of the use of force, that constituting an armed attack, with other less grave forms of the use of force.[6] The Court also noted that there were activities that would constitute a breach of the principle of the non-use of force and an intervention in the internal affairs of a State that would be a conduct that was wrongful but of less gravity than an armed attack.[7]

74. With respect to ICTs, the group of governmental experts established pursuant to General Assembly resolution 73/266 solicited voluntary national contributions from participating governmental experts on how international law applies to the use of such technologies by States.[8] In many of the contributions, the law on the use of force and the right to self-defence were addressed:

(a) States variously considered that an act using ICTs can constitute a use of force if it (a) has the same effects as a use of force using physical means;[9] (b) causes physical damage, injury or death; (c) targets critical infrastructure and results in serious damage, injury or death; (d) causes severe disruption to the functioning of the State, including the sabotage of governmental or private power grid or telecommunications infrastructure; or (e) targets a State's financial and banking system, or other operations causing widespread economic effects and destabilization;

(b) States variously considered that an act using ICTs can constitute an armed attack if it (a) causes physical damage, injury or death, directly or indirectly, that is similar or equivalent in its scale and effects to an attack with conventional means and that exceed a threshold of gravity to constitute a use of force, or that presents an imminent threat thereof; (b) severely damages or disables a State's critical infrastructure or functions or causes sustained and long-term outage of such infrastructure or functions; (c) is attributable to a State; and (d) causes harmful effects outside the territory of the attacking State;

(c) Many States separately addressed other aspects of Article 2 (4), including prohibited interventions and violations of sovereignty, and noted that acts using ICTs that may not amount to a use of force may nonetheless qualify as a prohibited intervention or a violation of sovereignty.

75. With respect to outer space, recent United Nations bodies have addressed the ways in which international law applies to acts using or affecting space systems:

(a) The group of governmental experts established pursuant to General Assembly resolution 72/250 considered the application of the right to self-defence in outer space as one of the thematic areas that could be addressed in a possible legally binding instrument. Although the group was ultimately unable to agree on a substantive report, the report by the Chair to the open-ended

[6] See International Court of Justice, *Nicaragua v. United States of America*), ICJ Reports 1986, Merits, Judgment, 27 June 1986, para. 191.

[7] Ibid., para. 247.

[8] The voluntary national contributions submitted by the respective participating governmental experts and are contained in document A/76/136 in the language of submission only.

[9] To ensure the consistency of terms used throughout the present report, the term "physical" is used where various States refer instead to "kinetic" effects, taking into account that the physical impacts of conventional weapons used in other domains are distinguishable by having kinetic, explosive and thermal effects.

consultative meeting held in January 2019 provides insight into the views of the experts represented on the group (A/74/77, annex II). There was no dispute that international law and the Charter of the United Nations in particular apply in outer space. There was some convergence on the notion that it would be useful to avoid any attempt to determine what constitutes the use of force in outer space pursuant to Article 51 of the Charter and to focus instead on the regulation of behaviour as may be agreed by States. This included the possible prohibition or limitation of harmful or hostile acts involving space objects. There was no single view on, inter alia, how to deal with intentional interference with or disruption of a space object that does not result in permanent damage;

(b) In their submissions to the report of the Secretary-General pursuant to General Assembly resolution 75/36, States provided examples of actions and activities that could be considered either responsible, irresponsible or threatening (A/76/77). A number of States expressed concern over so-called hybrid operations, in which systems are intentionally targeted to disrupt their services using means that fall below what a State could consider the threshold for the use of force. As an element for norms, rules and principles of responsible behaviours, it was suggested that States consider agreement upon an obligation to refrain from the use of force leading to the intentional destruction of space objects;

(c) The open-ended working group discussed issues relating to the application of Articles 2 (4) and 51 of the Charter as well as the application of other bodies of international law to the outer space domain (A/AC.294/2022/3). It was suggested that States should reach a common understanding of what constitutes a use or threat of use of force and an armed attack in the context of outer space. One means of doing so could be to focus primarily on the effects, impacts and consequences of acts affecting space systems as opposed to focusing exclusively on specific capabilities. It was also suggested that States should reach a common understanding of undesirable acts that fall into a so-called “grey area”, beneath the threshold for what is commonly considered to be a use of force or an armed attack.

76. With respect to the use of armed uncrewed aerial vehicles, studies by the Office for Disarmament Affairs[10] and the United Nations Institute for Disarmament Research have described challenges posed by such systems, in the light of observed trends in their use resulting from their unique characteristics. It was noted, for example, that armed uncrewed aerial vehicles have been used to apply force with such a low level of intensity that it was unclear whether or not the act exceeded the threshold to be considered an armed attack. Both studies supported the development of agreed measures by States to increase transparency, oversight and accountability with regard to armed uncrewed aerial vehicles.

IV. Conclusions and recommendations

77. Many of the developments addressed in the present report are the subject of recent or active multilateral deliberations within the framework of the United Nations or elsewhere. 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.

[10] See www.un.org/disarmament/publications/more/drones-study and https://unidir.org/publication/increasing-transparency-oversight-and-accountability-armed-unmanned-aerial-vehicles.

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

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

80. Furthermore, it is recommended that processes to review the operation of disarmament treaties and all relevant United Nations disarmament bodies devote specific time to keeping up to date with all relevant work undertaken in other processes and bodies that address issues connected with developments in science and technology.

81. It is recommended that reports containing updates to the information in the present report continue to be submitted 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.