UN General Assembly First Committee high level exchange on the current state of affairs in the field of arms control and disarmament and the role of international organizations with mandates in this field

"The implications of emerging technological developments on disarmament and non-proliferation"

Remarks

by

Ms. Izumi Nakamitsu

High Representative for Disarmament Affairs

11 October 2017
New York
Mr. Chairman, Ambassador Bahr Al-Uloom,
Distinguished delegates,
Excellencies, ladies and gentlemen,

At the outset I want to warmly welcome my colleagues from across the UN disarmament and non-proliferation system – Mr. Michael Møller, Secretary-General of the Conference on Disarmament; Mr. Xolisa Mabhongo, International Atomic Energy Agency; Dr. Gareth Williams, Organisation for the Prohibition of Chemical Weapons; Mr. José Rosemberg, Preparatory Commission for the CTBT Organization; and Mr. Luiz Filipe de Macedo Soares, Agency for the Prohibition of Nuclear Weapons in Latin America and the Caribbean – and thank them for joining this event.

Our topic today is one that is increasingly moving to the forefront of our thinking and our deliberations. As the Secretary-General noted in his address to the General Assembly last month, “technology will continue to be at the heart of shared progress” but also that the “dark side of innovation” is a threat we must confront, and one that has “moved from the frontier to the front door”.

In discussing emerging technological developments we are considering a range of technological innovations that are already revolutionising transportation, healthcare and manufacturing.

However, the same innovations also have either military applications or can be re-purposed for malicious intent. Technological innovations with possible implications for peace and security include enabling technologies – such as machine learning or information and communications technologies; others are dual use, such as biotechnology and additive manufacturing, and specific weapons technologies, such as new types of long-range precision delivery vehicles and armed unmanned aerial vehicles.

Together these innovations have the long-term potential to change how wars are fought and increasingly place civilians in harm’s way. Take, for example, the “enabling” nature of cyberspace, which means that ICT-enabled critical infrastructure, ranging from healthcare facilities to power grids to nuclear facilities, are vulnerable to attacks because they rely on computer networks to function.

In the military domain, long-term effects could include destabilising arms races as advanced States seek to build or negate perceived advantages. We can already see echoes of this in recent statements about artificial intelligence and defence strategies based on unmanned and autonomous technologies.

In the future, technological innovations could potentially lower the threshold for armed conflict due to perceptions of casualty-free warfare or due to the accelerated pace and enhanced scale of conflict leading to a failure of escalation control.

In the near-term, questions are being voiced about how these innovations could impact stability, and their abilities to conform to international humanitarian law and human rights law. Serious concerns have been raised about attribution and accountability, especially in the context of cyberattacks and autonomous weapons systems.
It is also conceivable that, due to some of these technologies’ portability and commercial availability, these innovations could increase the risk of proliferation, including to non-state actors.

Unlike previous military-technological revolutions such as nuclear weapons, often it is the cumulative impact of largely civilian technology that we now need to be aware of. I have mentioned before the possibility of a networked autonomous drone using space-based systems for guidance and facial-recognition software for targeting.

There are two other aspects of this technological revolution that need to be highlighted. First, these innovations are being driven largely by the private sector, not by governments, and the technologies they are developing are largely ungoverned. If we are to address the challenges they pose, we need to devise mechanisms for bringing industry inside the tent.

And second, the technological revolution is occurring at a time of growing geopolitical instability and inflamed regional disputes. The combination of this combustible situation with potentially revolutionary new weapons could have grave consequences for peace and security.

Excellencies, ladies and gentlemen

The UN system is already attempting to deal with some of these innovations across various forums. Secretary-General Guterres has repeatedly expressed his concerns about what he calls “frontier issues”, which include lethal autonomous weapon systems, cyberattacks and developments in biotechnology, and has tasked the UN system with developing strategies for how it can best help “we the peoples” of the UN Charter to address them.

In the disarmament machinery, action is already being taken. The Convention on Certain Conventional Weapons (CCW) will convene in November a formal inter-governmental expert process to deliberate on how to approach lethal autonomous weapons systems. As many of you know, there have also been five General Assembly mandated groups of governmental experts on information and communications technologies.

Even the United Nations Disarmament Commission, mostly known in recent times for its inability to fulfil its mandate, this year held an informal exchange on the proposal for a new item on the implementation of transparency and confidence-building measures in outer space activities, for the purpose of preventing an arms race in outer space. The Secretary-General’s Advisory Board on Disarmament Matters has proven a valuable incubator for ideas on how to address the challenges posed by emerging technologies.

It was the Advisory Board that examined the issue of lethal autonomous weapon systems in 2013, recommending coordinated efforts in an existing forum such as the CCW.

In 2014, the Board considered armed unmanned aerial vehicles, leading to a study by ODA that presented ideas for improving transparency, oversight and accountability in the development, acquisition, stockpiling, transfer and use of armed UAVs. I welcome the
follow-on initiative by UNIDIR to carry forward multilateral dialogue on this issue and look forward to its recommendations on how it could be taken forward in a formal setting.

In 2016, the Board considered the development of conventional long-range weapons. Noting that such weapons “could eventually upset strategic stability”, the Board called for a study to inform further Member State deliberations, including on possible recommendations for arms control measures. Work on this study is underway.

Most recently, the Board discussed the impact of artificial intelligence on international security, highlighting the need for further study of the issue.

As various parts of the UN system grapple with this issue, I think we all agree that our work needs to pick up the pace, achieve more depth in analyses, and obtain broad and strategic overview on the interlinkages of the challenges we face.

Excellencies, ladies and gentlemen

Normative considerations must keep pace with technological developments. However, it is equally important that once norms are developed they are fully implemented.

In this context, the need to prevent the potentially destabilizing effect of cyberattacks should be of paramount concern. It is estimated that by 2020, the number of people online will double to four billion, with around 30 billion devices connected to the internet. Incidents such as that involving the “Wannacry” ransomware, which reportedly affected around 200,000 systems in over 150 countries, demonstrate the international and interconnected impact of cyberattacks.

Deliberations on these issues in the UN are at a critical juncture as the most recent Group of Governmental Experts was not able to reach consensus on a final report. However, it is important to keep in mind that we already have three substantive reports from previous GGEs with important assessments and recommendations upon which to build our work.

These consensus reports have laid the foundation for a non-binding framework that can help prevent and mitigate the prospect of offensive cyber operations. Chief among these norms is an enduring commitment to an open, secure, stable, accessible and peaceful ICT environment. What matters now is that all States seek to respect this framework through their actions in cyberspace.

Excellencies, ladies and gentlemen

It should be made clear by today’s presentations that within the UN framework we are making progress in attempting to deal with the challenges posed by emerging technology. But we cannot afford to rest. The pace of technological innovation outstrips the pace of international deliberations, arguably by orders of magnitude. Likewise, the pace of investment in innovation dwarfs investment in norm-building. As I noted earlier, many of the potentially game-changing innovations impacting our work are currently ungoverned.

So, moving forward I pose the following questions to Member States.

First, do we have a clear enough understanding of the ramifications of these new weapons – including their combined effects – including how they will be used?
Second, what is the scope of governance or regulation required to ensure they do not become destabilising, are not used either for unintended purposes or in contravention of international law?

Third, in this context, is the current system fit for purpose or do we need to consider new instruments and initiatives? What new confidence-building and transparency measures can we develop? Are we properly utilising all the tools at our disposal?

Fourth, how can these technologies be governed without stifling innovation or inhibiting technology transfers that could enable sustainable development?

Fifth, what are the opportunities for our work presented by these technologies? The benefits for verification stand out, but there are others, such as enhanced detection of WMD use and the ability to mark and trace conventional weapons.

Finally, are we moving fast enough and are we doing so in a way that addresses these challenges strategically and holistically?

Excellencies, ladies and gentlemen

The emergence of lethal autonomous weapons systems, cybersecurity issues, synthetic biology, UAVs and other new challenges add to the already immense load borne by the disarmament and non-proliferation machinery.

These issues will only become more central to our work, especially as they begin to impact historic areas such as conventional and WMD arms control. It is, therefore, vital that we keep pace with new challenges in ways that are open, transparent and based on inclusive dialogue.

In this connection, I feel obliged to end my remark today by repeating some of the messages I gave to you in the informal exchange with you yesterday. The work in the areas of arms control, non-proliferation and disarmament has become more critical than ever, in the face of on-going fundamental changes in the international security environment. Various parts of the disarmament machinery need to function effectively as an integrated system contributing to the maintenance of international peace and security in the 21st century. Conference on Disarmament has to come out of the long stalemate. I hope that each of you will take the important responsibilities of member states well beyond the confines of this room, and traditional resolutions, and create dynamism for innovation and momentum.

I stand ready and look forward to working with you on all disarmament and non-proliferation challenges, including ensuring that rapid advances in technology work for the benefit of humanity, not against it.

Thank you.