UNODA United Nations Office for Disarmament Affairs

Keynote speech by the High Representative for Disarmament Affairs, Ms. Izumi Nakamitsu, at high-level event on frontier technologies for accelerating Sustainable Development

(Delivered in conjunction with a panel discussion on "New technologies = opportunities – What about the risks and threats?")

New York
5 March 2019

I would like to start by thanking the permanent mission of Finland, as well as my colleagues from OICT and UNICEF, for organizing this important and timely event.

Throughout today we have heard of the many benefits frontier technologies, and especially artificial intelligence, can provide to better the lives of all inhabitants of our planet Earth.

Sadly, in my capacity as High Representative for Disarmament Affairs, I am forced to focus on the "dark side", that is, the negative applications of new technologies, or – to be blunt – the applications of technologies in warfare.

I want to make clear from the outset that the potential risks posed by new technologies should in no way discourage pursuits in technological developments or be used as an excuse to inhibit innovation. Quite the contrary.

In fact, we at the United Nations are also interested in promoting and facilitating the beneficial applications of science and technology for achieving our aim to create a safer and more secure world.

Therefore, it is our key challenge to ensure that we can understand, manage and mitigate the potentially negative implications of various technological advancements without hampering social and economic development and the pursuit of basic scientific research and exploration.

So before diving into the risks, I would like to begin on an optimistic note. Today's rapid digital and technological transformations inspire hope of immense benefits that can elevate the human condition everywhere. We can see a future transformed by artificial intelligence, edited genomes, autonomous cars, stateless currencies and private space travel. I'd like to live long enough to see that.

These new technologies hold incredible promise for human welfare. They offer us powerful new ways to achieve our shared commitments to each and every one of the Sustainable Development Goals.

Within the international security domain, AI also shows significant potential to do good.

For example, AI can be used to scan networks and detect abnormal activity at much greater speeds and on a larger scale than if these tasks were performed by humans. It can support

system administrators by monitoring large amounts of traffic and recognize those activities that require action. In many cases, even the responses to such incidents can be automated.

To reduce nuclear risks, AI-enabled technologies could allow States to analyze large amounts of data to verify critical information, while global ICT-networks facilitate real-time communications that could reduce the risk of miscommunication.

As for blockchain, there is ongoing work within the International Atomic Energy Agency (IAEA) to explore whether shared ledger technology can be applied to the confidential reporting on certain safeguards on nuclear materials.

Ladies and gentlemen,

Despite these advantages, the inherently *dual-use* or *general-use* nature underlying many of these technologies poses significant risks.

Science and technology are being weaponized, and as such, they have the potential to undermine international peace and security. This is exacerbated by our increasing reliance on AI and other technologies. Think about the ever-expanding Internet of Things: smart cities, self-driving cars and intelligent industrial control systems.

This means that the security dimensions of these technologies stretch beyond SDG Goal 16 on Peace and Security. Take for example SDG 9 and the need to ensure the protection and resilience of infrastructure, industry and innovation. And in the context of Goal 11, consider the importance of keeping smart cities safe and resilient.

Developments in artificial intelligence are driving interest in autonomy in weapons and other military systems. The possible implications are vast and multi-dimensional.

Although there is no precise definition, the term “autonomous weapons” is broadly used to refer to any weapon that could select and engage targets without human intervention. Such a system would use AI to complete tasks that had previously been conducted by humans.

There are already weapon systems in service today with such capabilities, although deployments of these systems currently remain largely limited to specific environments, such as the open seas, far from civilian populations.

The trend towards increasing autonomy in the critical functions of weaponry has been raising concerns on multiple fronts for several years now.

There could be serious consequences for international security: this trend could lead to a new and destabilizing arms race. It could lead to perceptions of casualty-free warfare, lowering the threshold for armed conflict. The speed at which AI-enabled weapons systems could operate will place increasing pressure on human decisionmakers, with negative implications for escalation control.

The prospect of fully autonomous weapons also raises ethical and legal concerns.

While technological advances may improve accuracy and thereby reduce collateral harm, autonomous systems currently remain far from the point where they can reliably make decisions and judgments necessary for compliance with international law.

Moreover, it has been argued that no weapon system could ever be capable of performing the judgments required to conform with humanitarian principles and that the application of IHL is predicated on human judgment and responsibility.

The convergence of AI with other digital platforms could also raise concerns. AI can be applied to write malware that can learn the normal patterns of business operations and security protocols and thereby evade detection of its malicious activity.

The other way around, cyberattacks can compromise the reliability and safety of AI-applications in different fields. With AI being such a large part of everyday life, this can have far-reaching consequences. Consider the effects on the Internet of Things: there has already been an incident with terrorists that hacked drones to make them attack a target in a so-called *swarm*.

On the battlefield, these new vulnerabilities introduce new dangers such as the possibility of third-party State or non-state hackers with malicious intent seeking to incite conflict.

Just as in cyber defence, *scalability* is a key factor in cyber threats. A human hacker will still be most crafty in understanding a network and intelligently manipulating a system. However, heavy damage can be inflicted by automating this process; it is less labor-intensive and more cost-effective.

Ladies and Gentlemen,

To mitigate the potential harm caused by these technologies to international security, **technical solutions alone are not enough.**

International security requires mutual trust in rules, principles and norms. It is therefore imperative that the international community reinforces and adheres to emerging normative frameworks guiding the use of technology.

In that context, UN Secretary-General António Guterres has made a priority of ensuring the peaceful use of Science and Technology and especially ICTs.

At the 2018 Web Summit, the Secretary-General stated unequivocally that autonomous weapons with the discretion and capacity to take human lives would be politically unacceptable, morally repugnant and should be banned.

In his Agenda for Disarmament, released in May of last year, he pledged to support the efforts of States to elaborate new measures to ensure that humans remain in control over the use of force at all times.

Intergovernmental discussion on this topic has been taking place within the Geneva-based Convention on Certain Conventional Weapons (CCW) since 2014, and in a formal group of governmental experts since 2017.

This group produced a consensus outcome at the conclusion of its 2018 deliberations, including agreeing to a set of 10 possible guiding principles.

In 2019, I hope the group can build on this to narrow in on commonalities and agree on a productive way to take its discussion forward to respond to the concerns I touched upon earlier.

Ladies and Gentlemen,

I believe that in order to find real solutions, we must look beyond the scope of international organizations and intergovernmental deliberations.

At the end of the day, the driving force behind these technologies is *innovation.* And the history of scientific invention is marked by brilliant minds who never thought their research would be used to do harm.

In this context, it is important to highlight another commitment made by the Secretary-General in his Agenda for Disarmament: to engage and work with all stakeholders, including researchers, industry, and educators to encourage responsible innovation of science and

technology, and to ensure its application for peaceful purposes in conformity with the principles and objectives of the United Nations.

I believe it is vital to encourage a better application of 'foresight' – that is, the ability to consider plausible ways technologies, systems and features *might* be used, not just how it was meant to or *should* be used.

The work of the Office for Disarmament Affairs is only one part of the larger effort by the international community to deal with the risks and challenges posed by the rapidly advancing technologies.

I am excited to hear from the distinguished panel who will undoubtedly shed *their* light on the looming threats stemming from science and technology.

Thank you.