



the 2019
**innovations
dialogue.**

**DIGITAL TECHNOLOGIES &
INTERNATIONAL SECURITY**



UNIDIR

UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH

the 2019 innovations dialogue.

*Recognizing the interest of the international community to learn about developments in science and technology of relevance to international security, in December 2018 the United Nations General Assembly requested the United Nations Institute for Disarmament Research (UNIDIR), to convene a one-day informal seminar on the role of science and technology in the context of international security and disarmament, "in order to facilitate dialogue among relevant stakeholders on current developments in science and technology and their potential impact on international security and disarmament efforts."*¹

Through the generous support of the Governments of Germany, India, Qatar and Switzerland, UNIDIR convened the **2019 Innovations Dialogue on Digital Innovations and International Security** on 19 August 2019 at the Palais des Nations in Geneva.

CONTEXT



Tatiana Valovaya, Director-General, UN Office at Geneva & Renata Dwan, Director, UNIDIR

The world we are living in today is more interconnected than ever before in human history. It is clear that no one country alone can tackle the problem of the potential negative impact of scientific and technological advances on international security.

TATIANA VALOVAYA
DIRECTOR-GENERAL,
UN OFFICE AT GENEVA

As innovations in science and technology transform every aspect of our lives, societies, economies and social structures, States and policymakers seek to capitalize on the potential revolutionary benefits of these innovations, and to mitigate the risks, harms, and unintended consequences that they may pose. This is true in every domain, including in international security, disarmament and arms control.

However, as innovations in science and technology with implications for international security can arise from a vast range of disciplines—from physics, engineering, and materials sciences, to synthetic biology, machine learning and robotics just to name a few—**keeping abreast of new breakthroughs** of relevance to disarmament and international security practitioners is particularly challenging. Horizon scanning for the international security implications of specific innovations inevitably takes a back seat to current arms control and disarmament commitments and challenges.

UNIDIR's inaugural Innovations Dialogue took as its theme **digital technologies**, at a time when the implications of advances in this domain have dominated high-profile initiatives and multilateral debates. Earlier this year the Secretary-General's High-Level Panel on Digital Cooperation recommended the



Opening of the 2019 Innovations Dialogue

need for identifying and strengthening norms for responsible uses of technology, in order to build trust, security and stability in a world characterized by digital interdependence.² Other aspects of digital technologies are currently being explored in multilateral processes, including the sixth United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, the Open-Ended Working Group in the field of information and communications technology, and the ongoing discussions on Lethal Autonomous Weapons Systems within the framework of the Convention on Certain Conventional Weapons.

While making important contributions to international security, these discussions have narrow or limited mandates, tend to focus on current or near-term technological developments, and have varying levels of engagement with other stakeholders, such as the private sector and the technical community. And despite these efforts, the Secretary-General has warned that “The scale, spread and speed of change made possible by digital technologies is unprecedented, but the current means and levels of international cooperation are unequal to the challenge.”³

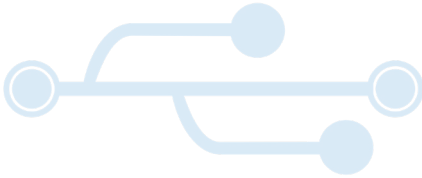
Through a forward-looking lens, focusing on new issues and converging technologies that are not currently on formal international security and disarmament agendas, the Innovations Dialogue aims to **assist Member States in navigating the rapid pace of technological change by providing a platform for open and inclusive discussion.**

The scale, spread and speed of change made possible by digital technologies is unprecedented, but the current means and levels of international cooperation are unequal to the challenge.

ANTÓNIO GUTERRES
UN SECRETARY-GENERAL

THE INNOVATIONS DIALOGUE PROMOTES...

... new approaches by building shared understandings of complex topics



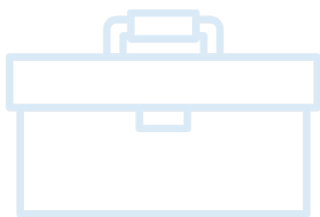
Through fact-based, balanced discussions, the 2019 Innovations Dialogue considered the beneficial applications as well as the challenges or risks posed by **quantum computing, distributed ledger technologies, the Internet of Things, and artificial intelligence**.

... new relationships by engaging different stakeholder groups



The rapid development, deployment and exploitation of digital technologies have extended the range of actors and their influence in the security space. In the absence of normative and legal frameworks, **States'** pursuit of strategic advantage by being a first mover in the military applications of digital innovations can be perceived as destabilizing and potentially trigger technology 'arms races'. The **private sector** has been in the lead of digital innovations, yet the roles and responsibilities of private stakeholders in the security implications of their products and services are not fully understood or shared. **Scientists and technologists** design and develop beneficial and multi-purpose innovations, but consideration of the implications for international security and stability of their work are not necessarily part of their training, standard practice or risk assessments.

... new tools through consideration of how to leverage innovations for disarmament objectives



There are also opportunities for the international community to **harness digital innovations to address existing disarmament challenges**. In addition to military applications, these innovations also hold promise for novel means to support arms control and disarmament objectives, such as ledger technologies and end-to-end digital traceability platforms that can increase accuracy and transparency in record keeping, tracking and verifying data concerning stockpiles, imports, transfers, exports, and supply chains of weapons and dual-use items.

This report is a summary of the themes and key insights of the 2019 Innovations Dialogue. Conference materials, including videos of the livecast on UN Web TV, speakers' presentations, and the agenda of the event are available on **UNIDIR's website**.⁴

SUMMARY OF DISCUSSIONS

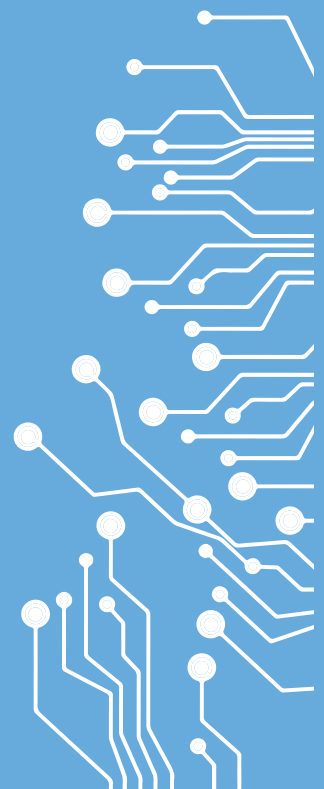
The inaugural Innovations Dialogue provided an open and inclusive platform to explore digital technologies and their implications for international security. The specific technologies discussed included quantum computing; distributed ledger technology (DLT); the Internet of Things (IoT); and artificial intelligence (AI).

This section includes a brief overview of each session of the Innovations Dialogue.⁵

DIGITAL INNOVATIONS & THE GLOBAL SECURITY LANDSCAPE

It is often difficult to imagine the potential ways in which **digital technologies could transform international security and stability** over the coming years, let alone what could be appropriate policy responses to them. Even when policymakers consider, for example, machine learning in conventional weapon systems or when the focus is on a singular, stand-alone technology, discussions may seem abstract and disengaged from the context of—and implications for—international relations and security. In order to set the scene for these discussions, attendees were invited to look through the gaze of a futurist and imagine how over the coming decade digital innovations could transform relations among States, the private sector, and technical communities. They were asked to consider a fictional scenario,⁶ where quantum computing, DLT and IoT are at the centre of daily lives, societies, financial sectors and even international security and stability. The scenario presented the socio-economic benefits of dual-use innovation in tension with a race for technological supremacy, shifting strategic alliances, and changes in the balance of power among technological ‘Haves’ and ‘Have Nots’.

Although the scenario was fictional, ongoing **developments in digital technologies certainly warrant the arms control and disarmament community’s attention today**. While understanding these innovations and their implications for security and stability may seem daunting, this session highlighted the wealth of existing resources and various communities of actors working on different facets of these questions—from normative frameworks, to legislation and regulation, to national and international standards. The arms control and disarmament community is only one among many that are grappling with how to maximize the considerable potential of digital innovations while minimizing or mitigating the risks and potential harms. There are many actors in the private sector, industry, the technical community, and academia that work on these cross-cutting issues. Bringing these actors together in inclusive multi-stakeholder dialogues offers an opportunity to foster exchange of knowledge and perspectives, infuse new thinking and solutions, develop common understandings and vocabulary, and see how each community can contribute to the objectives of peace and security.





Lim May-Ann, Asia Cloud Computing Association

TECH TRACKS

The United Nations can play a central role in promoting greater understanding of implications posed by developments in science and technology.

ANTÓNIO GUTERRES
UN SECRETARY-GENERAL⁸

The Tech Track breakout sessions offered participants an introduction to a specific technology: quantum computing, DLT or IoT. Co-led by a technical expert and an international security policy expert, these interactive sessions provided an initial appreciation of the risks and benefits of these innovations. What are they? How do they work? What implications may their development and diffusion have for international security and stability?⁷



QUANTUM COMPUTING

Quantum computing leverages quantum phenomena of superposition and entanglement to achieve **exponential increases in computing capabilities**—making quantum computers much more powerful compared to today's computers that use a binary system of 0s and 1s. Quantum computing enables calculations of a large quantity of data at once, without being constrained by the physical limits of classical binary computers. Due to the specific conditions necessary to preserve quantum particles and the overall complexity of the technology itself, only a few States and industry actors are able to dedicate the resources necessary to conduct successful research in quantum computing.

Even though quantum computing is still in its early stages of development, there are many promising practical applications for international security and disarmament. The unprecedented computational capacity promised by quantum computers could be used to **boost machine learning capacities** in military applications, including in planning and predictive analytics. Furthermore, quantum computers could **conduct modelling and simulation** at a new scale and level of complexity.

Due to their ability to do calculations of massive amounts of data quickly, quantum computers **could break the most complex cryptographic codes** written by classical binary computers. As a result, many of today's encryption algorithms will no longer ensure effective protection of data once a sufficiently powerful quantum computer is built. In addition, quantum computing provides the potential for **far stronger encryption** tools and techniques than currently exist. The ability to create stronger encryption than one's adversaries, as well as the ability to break the encryption of others, is equally attractive to responsible actors as it is to malicious ones.



Patrick Towa, IBM Research

The opportunities promised by quantum lead to **increasing investments and mounting competition**. However, as stated, only a few States and industry actors are likely to be in a position to significantly invest in quantum computing research. A potential strategic implication might be a growing gap in strategic capabilities between States possessing quantum computers and those that do not.



FOR MORE INFO...

including a recording of the session, explainer videos and suggested readings, visit:

bit.ly/UNIDIR-Innovations

DISTRIBUTED LEDGER TECHNOLOGY

DLT is based on a **distributed, decentralized digital data repository** (a ledger) in which all information is added in a 'block' and stored within a chain of transactions. Once the information has been added and validated, it cannot be altered or deleted without breaking that chain.

The data stored in a distributed ledger is **immutable**, due to multiple layers of encryption, which makes the data tamper proof. The ledgers themselves are **decentralized**—each ledger is supported by all its participants, and transactions adding new data to the ledger are made on a peer-to-peer basis.⁹ The **distributed nature** of the technology means that ledger participants store copies of that ledger's data, thus DLT offers **resiliency** to equipment failures, cyberattacks and other security incidents. Distributed ledgers can be **permissionless** (in which anyone can participate without restriction) or **permissioned** (where one needs to be authorized by an administrator to participate).¹⁰

Due to a combination of these properties, DLT is sometimes described as a **trust machine**¹¹—a tool enabling trust in an environment where counterparts do not trust, or even know, each other. These properties make DLT particularly attractive for contexts or processes with a limited number of participants (e.g. States Parties to a regime or an agreement), where sensitive information is at stake (the ledger can provide proof-of-existence of such information without revealing its actual content), or where there is a lack of trust or transparency among parties.

Practical applications for international security include **monitoring and verification** of nuclear safeguards regimes and agreements; strengthening **export controls** regimes and compliance procedures; and **tracing** the manufacture, supply chain, transborder



Suzana Maranhão, ITU Focus Group on Application of DLT

shipping or export of dual-use items, sensitive materials and arms.

DLT is not flawless. It does not, for example, guarantee that information is complete and accurate before it is loaded to the ledger. In addition, the infrastructure (platform), the software and the data itself are all elements that could be compromised under certain conditions. Trust in the ledger ultimately depends on the security and integrity of the data that is contained within it. As such, DLT could be a **useful addition to existing tools and processes** rather than a replacement.

FOR MORE INFO...

including a recording of the session, explainer videos and suggested readings, visit:

bit.ly/UNIDIR-Innovations



INTERNET OF THINGS



Madeline Carr, PETRAS, Merel Ekelhof, UNIDIR & Jan-Peter Kleinhans, Stiftung Neue Verantwortung

The IoT can be described as “a global infrastructure for the information society, enabling advanced services by inter-connecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”¹² It enables **connectivity** between devices (sensors, actuators, microchips, etc.) embedded in various objects and infrastructures. This connectivity allows these devices to generate, exchange and consume data without—or with minimal—direct human intervention. This is why IoT-connected devices are often called ‘**smart devices**’. Through universal connectivity, IoT enables an unprecedented level of **automation and efficiency**.

Practical applications for international security include **automated systems** used for fire-control systems, **monitoring** storage of ammunition, smart military bases (using the concept of smart cities), swarm **networking** within IoT-based systems, and improvement of command and control through the **processing** of data collected by various sensors.

Because it increases connectivity among

devices, IoT expands the **attack surface** of connected ‘smart’ ecosystems, creates **interdependencies**, and increases the **risk of cascading effects** in the event of serious security incidents with IoT-connected systems.

For many years the majority of common IoT devices (sensors, webcams, indicators, GPS trackers, etc.) lacked even the most basic security features, nor did they have a way to upgrade or to patch known security flaws. Networks of **compromised IoT devices** have been used as botnets to conduct powerful attacks against online services and even critical infrastructures. As dependencies on the IoT continue to grow, ensuring robust **security, interoperability** of standards, and understanding of the **shared responsibility** of designers, manufacturers, regulators and users to secure the IoT will become even more critical.



FOR MORE INFO...

including a recording of the session, explainer videos and suggested readings, visit:

bit.ly/UNIDIR-Innovations

DIGITAL INNOVATIONS FOR INTERNATIONAL SECURITY & DISARMAMENT



Panel discussion on digital innovations for international security & disarmament

Trial use and applications of digital technologies to very specific areas of international security and disarmament are starting to emerge. The purpose of this session was to explore some of these **current and near-term applications of digital innovations** through concrete examples. These use cases provided insights into how these technologies are currently leveraged for arms control and disarmament objectives and how these might be more broadly used in the future.

One example relates to applications of IoT in the defence sector. New chips integrated with AI result in **smarter chips that can execute the entire Observe–Orient–Decide–Act (OODA)¹³ loop at the sensor level** without, or with minimal, human intervention. While this may be highly contentious in some areas, such as weapons, smarter chips are already used in others, such as logistics (optimization

of maintenance, route etc.) and ammunition surveillance. A very specific use case in the area of ammunition is the ability to remotely monitor temperatures and humidity in stockpiles of ammunition and other explosive materials to ensure safe storage and to monitor shelf-life based on changes in conditions.

A second example is the use of DLT to contribute to the verification regimes for the prohibition of chemical weapons. DLT would allow a more streamlined and verifiable declaration process between various actors involved in the transfer of chemical materials. In current practices, transfer discrepancies may occur owing to contradicting declarations made by States. This lack of harmonization of the convention among States Parties may even point to a violation of the Chemical Weapons Convention. DLT could be leveraged to improve **verification and transparency**, potentially building trust and confidence among actors.



Benjamin Ang, Nanyang Technological University

Within the field of nuclear safety, DLT could be used to provide a secure and consistent method of archiving national nuclear information. In addition, DLT could also help participating stakeholders in accessing the latest version of amendments to shared databases. This has the potential to **streamline and strengthen safeguards by facilitating the traceability of data**, the verification of transactions and real-time detection of unauthorized access and diversion, while complying with IAEA regulations and standards. As industry and governments become more digitized, DLT offers a novel technological solution for sharing online transmissions in a more secure manner.

Quantum algorithms could be used to **protect sensitive or classified data**. This could be applied by the financial sector (e.g. banks protecting data), but also by governments and the international community (e.g. protecting sensitive data regarding ongoing operations, weapons development and other classified information). One way to protect that data is to use quantum key distribution. A quantum encryption key would be truly random, could be changed constantly, and would make it impossible to eavesdrop without detection.



As applications or pilots projects are already starting to emerge in very specific areas, it is important to explore current or near-term applications of these digital innovations through concrete examples and use cases.

GIACOMO PERSI PAOLI
UNIDIR

FIRESIDE CHAT ARTIFICIAL INTELLIGENCE & DATA



Kobi Leins, University of Melbourne, Lydia Kostopoulos, moderator & Arun Sukumar, Observer Research Foundation

Through their discussions within the Convention on Certain Conventional Weapons framework on Lethal Autonomous Weapons Systems (LAWS), the international community has begun to consider the role of artificial intelligence (AI) and machine learning in conventional weapon systems. However, AI impacts international security in a number of domains, going far beyond LAWS. A sustained conversation has yet to take place on the international security implications of AI beyond weapon systems, and particularly on the role of data in enabling AI applications therein.¹⁴

The fireside chat recommended that a useful point of departure for this conversation would be to recognize that **AI should not be discussed as a singular technology**, but rather as made up of a variety of elements, including data, sensors, algorithms, and actuators—as well as different approaches to machine learning. It was suggested that a more nuanced conversation about AI would start from consideration of choices about algorithmic design and data as well as greater awareness about its limitations and weaknesses.

Speakers underscored that **understanding the possible functions and value of data**

is of primary importance for governments and other stakeholders—and this awareness should precede racing to adopt AI-based ‘solutions’ as well as policy or regulatory decisions on how data is to be generated, used, shared or sold. Increased consultations within governments are also required to enable policy coherence. For example, a transportation department collecting data on traffic flows and vehicle registration might share or sell that data without consulting with the Ministry of Information and Communications on technical issues or Ministries of Interior and Foreign Affairs on potential security concerns.

Lastly, in addition to acknowledging the complexity of the various elements comprising AI, speakers noted that there are **variations in national approaches to AI** that shape not only AI-related policy, but also decisions about algorithmic design, policies about data collection and privacy, and principles about responsible uses of AI. In many ways this diversity might be considered a strength—with expertise widely spread there is no possibility of a ‘single point of failure’. Yet this diversity makes scaling up some of the beneficial applications of AI more challenging.

KEYNOTE & INTERACTIVE DISCUSSION

WITH IZUMI NAKAMITSU



Izumi Nakamitsu, UN High Representative for Disarmament Affairs

Discussions throughout the day demonstrated **the importance of multi-stakeholder dialogue to comprehensively address challenges and to maximize the benefits of digital technologies for international security and stability.** Izumi Nakamitsu noted that in today's increasingly digitized world where technological development moves at a very rapid pace, United Nations processes may not react quickly enough to find solutions, such as through the creation of multilateral normative and regulatory frameworks. One way for the disarmament and security community to keep up with the pace of change is by pursuing multi-stakeholder dialogue so as to obtain insights and understandings of what new technologies

are being developed and how they may apply, positively or negatively, to international security issues and processes. The United Nations should think more creatively about how to effectively use its convening power to engage different kinds of groups and actors in these discussions.

The High Representative also stressed the need for a deeper understanding of the existing disarmament resources before proposing new tools and mechanisms. **How can the international community better utilize, or perhaps adapt existing tools** to address the implications of digital technologies for international security policies, institutions and practice?

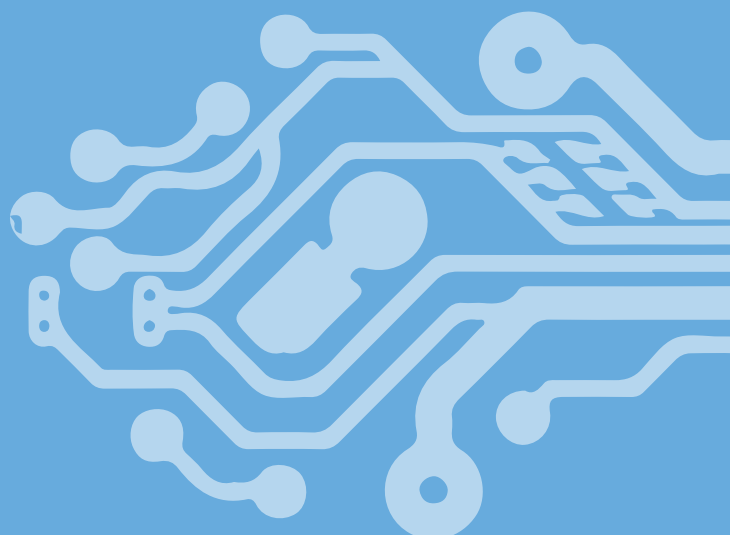


Renata Dwan, Director, UNIDIR

During the interactive discussion between the High Representative, the Director of UNIDIR and participants, there was broad agreement about the need for **nuanced and well-informed dialogue** through internal reflection and the questioning of outdated conceptions in the context of disarmament—such as the value of having expert discussions in silos. At the same time, participants cautioned against buying into the ‘**tech hype**’ narrative that any innovation in isolation ‘changes everything’.

The value of discussing specific use cases to demonstrate risks and benefits related to technological applications was considered particularly valuable. **Discussing concrete use cases** also helps to identify possible new avenues for control by considering not only what may work in theory but what would be the specific challenges of operationalizing these approaches in practice. Lastly, there was widespread acknowledgement that developing effective approaches and policies concerning the international security dimension of digital technologies cannot be achieved without **new relationships**.

The 2019 Innovations Dialogue concluded by encouraging participants to start building these relationships, reaching outside of their traditional networks to benefit from the experience, knowledge, creativity and tools of other communities. While promoting the importance of multi-stakeholder approaches borders on cliché, in the field of digital innovations it is not an option but a requirement.



KEY TAKEAWAYS



Elsa B. Kania, Center for a New American Security

While largely developed and produced for peaceful commercial applications, **digital technologies have significant defence and security applications.** These technologies have transformed warfare and continue to exert significant influence over military decision-making and international security thinking and practice. The next generation of digital technologies in the field of quantum computing, DLT, IoT and AI will push this change even further.

Digital innovations pose radical and novel implications—positive and negative—for international security and disarmament. While these technologies will create new risks and challenges that are important to address, it is equally important to explore the possible benefits—such as the potential of quantum computing in processing large amounts of data, for AI to find patterns and insights, for IoT to improve interoperability by sharing and analysing data through the cloud, and for DLT to build confidence in information when trust is lacking among actors.

The narrative around new innovations is often more informed by movies and media hype than by **fact-based assessments about technological capabilities and risks.** International deliberations and discussions would benefit from a more nuanced understanding of new technologies to inform both policy and diplomacy. The challenge is **how to equip the arms control and disarmament community with the necessary knowledge** to more easily comprehend and discuss the security implications of technological developments as an integral part of its portfolio.

Effectively harnessing the benefits and responding to the challenges that digital technologies present in the international security and disarmament context requires **new approaches, new relationships, and new tools.**

Until policymakers understand what data can be used for, they won't understand the benefits and risks of sharing data with the private sectors or others.

ARUN SUKUMAR
OBSERVER RESEARCH
FOUNDATION

NEW APPROACHES

TO ADDRESS A CHANGING SECURITY LANDSCAPE

Several characteristics of digital technologies—including the primary role of the private sector in their design and development, their dual-use nature, intangibility and potential replicability—means that traditional arms control tools may not be effective to address the risks they pose to international security. Therefore, **alternative approaches for 'digital arms control' may need to be explored**. These alternatives could include implementing novel regulatory frameworks, promoting the development of norms and standards in technical communities, prescribing taxes on specific technologies, or private sector incentivization, to name a few.

Deeper consideration is necessary of **how to incentivize the international community to cooperate** with specialized communities and the private sector on these issues when so many technologies are designed, developed and deployed by different actors and on infrastructures or in environments that are beyond any single State's jurisdiction.

In recognition of the unique characteristics of digital technologies—and in particular their transformative, cross-cutting nature—some States have **reorganized existing governance structures at a national level, or created entirely new ones**. Examples range from new ministries, such as a Ministry of Digital Economy and Society, new ministers or ambassadors for innovation, and specialized agencies and statutory boards, such as technology agencies.

Some have argued that the security and governance of digital technologies have been impeded by the relatively **chaotic state of standardization** for many technologies. For example, within the global IoT landscape, competition has resulted in a lack of interoperability and contributed to significant security gaps. Considerable work remains for international standardization bodies,

governments, manufacturers, operators and users in order to ensure more secure infrastructures.

Creating new approaches to respond to risks and uncertainties raised by digital technologies requires deeper **consideration of the relationship between data and technology**. While keen to seize the benefits of digital technologies—to derive actionable intelligence, create greater situational awareness, or improve interoperability—there is growing awareness concerning biases in data, data integrity in adversarial environments, and data protection.

Harnessing the benefits and mitigating the potential risks of digital technologies requires **urgent near-term improvements in cybersecurity**. Recent cyberattacks with financial damages in the billions, which have damaged or frozen critical infrastructure or essential services, have demonstrated that moving forward with increasingly powerful systems or ubiquitous digital devices that are built or implemented on insecure platforms or protocols could be considered increasingly irresponsible.

One narrative around digital technologies is that it is a 'winner-takes-all' race, even an 'arms race'. Rather than a race, it may be more helpful to consider it as a marathon, as **major breakthroughs will play out over decades to come**.

NEW RELATIONSHIPS

TO STRENGTHEN INTERNATIONAL SECURITY & DISARMAMENT

The **range of actors that influence international security and stability has widened** to include industry, civil society, academia, and the technical community. In order to create effective responses to harness the benefits and mitigate risks of digital technologies to international security, **new relationships** must be built among these stakeholders.

Advances in digital technologies are driven primarily by actors in the private sector and technical communities. The tremendous promise of digital technologies has led to **increasing investment** by both governments and industry, to **mounting competition** among such actors, and new types of **collaboration**. Due to the combination of government and industry actors involved, **more than ever before there are incentives to both cooperate as well as compete**. One participant called this “cooper-tition”.

The term ‘multi-stakeholder dialogue’ is likely too simplistic to adequately capture these new relationships and the types of interactions that are needed. It is not simply a case of including a greater number and diversity of experts. There may even be situations where the inclusion of more actors actually hinders progress or where multi-stakeholder approaches do not make sense. As such, there is a need to think more systematically about who needs to be at the table to address any given concern or to meet a specific objective.

It is unlikely that there will be one single model for building productive multi-stakeholder dialogue and thus finding the most appropriate format may require flexibility and experimentation with different arrangements.

Convening dialogue in itself might be insufficient. Meaningful cross-disciplinary discussion, particularly at its early stages, often requires actors that are skilled at **‘translating’ among different communities**—bridging different perspectives, facilitating understanding and helping to identify common vocabulary and language.

The Secretary-General has underscored the need to **engage with entrepreneurs and business leaders** and to promote the greater integration of experts, industry, and civil society into United Nations disarmament discussions.¹⁵

Member States and United Nations bodies would benefit from **engagement initiatives** that provide a continuous, inclusive and open relationship with various stakeholders in other communities.



We spend so much time discussing what we call the ‘dark side’ of technology, that we often forget to be techno-positive and remember that science and technology have been great enablers of peace and security, including disarmament processes. We need to think harder and more creatively about how we can harness the power of technological change.

IZUMI NAKAMITSU
UN HIGH
REPRESENTATIVE FOR
DISARMAMENT AFFAIRS



Building new relationships at the 2019 Innovations Dialogue

The Innovations Dialogue may be one platform through which policymakers can pursue multi-stakeholder engagement and a holistic approach towards the range of actors and tools that can contribute to international security and disarmament.

Rather than just occasionally drawing upon the expertise of actors external to the arms control and disarmament community, **a two-way dialogue should be fostered**. Not only will experts from outside the community be able to inform policy by sharing their knowledge and expertise on the state-of-the-art of digital technologies, policymakers can assist external actors by providing insights into existing international security-related contexts, policies, regulations, norms and tools.

A growing number of research organizations, centres and think tanks are **examining the risks and social and ethical implications of new technologies**. These voices could potentially offer new insights and considerations that go beyond those raised by policymakers, industry and the technical community.



NEW TOOLS

TO IMPROVE TRANSPARENCY, COLLABORATION & SECURITY

In addition to a variety of military applications—such as decision-support systems, intelligent systems improving situational awareness, and new approaches to cyber-defence and -security—there is great scope for the international community to harness digital innovations to support arms control and disarmament objectives.

The use of DLT is already being explored by a variety of international and national agencies. In the disarmament context, ledger technologies and end-to-end digital traceability platforms can **increase accuracy and transparency in record-keeping and track and verify the existence of data** concerning weapon stockpiles, imports, transfers and exports, and supply chains for weapons and dual-use items. Furthermore, DLT may have transformative impacts in regulatory bodies in building trust in the data- and information-sharing process due to the way in which DLT safeguards information. Therefore, even in an environment where there is distrust and sensitive information is being shared among various actors (e.g. States, institutions, and individuals), **DLT may offer unique solutions ensuring information integrity while protecting confidentiality**.

IoT enables an unprecedented level of automation and efficiency in business and technological processes across sectors and industries. In the military and security context this means the ability to **increase effectiveness** by collecting, analysing and sharing data from a wide range of platforms. For example, an IoT-integrated system can monitor, in real time, the safe storage of weapons, ammunition and explosive ordnance. Through the remote monitoring of temperature, moisture and diurnal cycling it is possible to **improve safe storage and handling of these items** and, as a result, adherence to international standards.

Quantum computing will **strengthen encryption and data protection**. The unprecedented computational capacity promised by quantum computers could be used to **boost machine learning and achieve further breakthroughs using AI**. This might include applications in support of strategic decision-making; strategic, operational, and tactical planning; and predictive analytics for defence and national security.

No single innovation is a 'silver bullet' or a solution in itself. In many circumstances they complement, strengthen or improve existing tools and procedures rather than replace them.

LOOKING FORWARD



Ambassador Peter Andreas Beerwerth (Germany), Brigadier General H.E. Hassan Saleh Al Nisf (Qatar), Renata Dwan (UNIDIR), Ambassador Felix Baumann (Switzerland) & Ambassador Pankaj Sharma (India)

This Innovations Dialogue is not the end of this conversation, but rather the start of a conversation that will be continued over the course of future years.

RENATA DWAN
DIRECTOR, UNIDIR

In this age of digital interdependence, no single State or community can identify and respond to the potential implications of digital technologies for international security. Events such as the **Innovations Dialogue** demonstrate that a number of communities of actors are working on different facets of these issues—and the disarmament community would benefit from drawing on the wealth of resources they represent.

Through its open and accessible format, with the active participation of policymakers, technical experts, industry representatives and civil society participants, the Innovations Dialogue demonstrated the value of convening different communities to explore how to promote international security through digital technologies. As part of its Security and Technology Programme, UNIDIR is committed to sustaining and strengthening these relationships through future editions of the Innovations Dialogue.

ACRONYMS

AI	artificial intelligence
DLT	distributed ledger technology
IoT	Internet of Things
LAWS	lethal autonomous weapons systems

ENDNOTES

1. United Nations General Assembly, "[Role of science and technology in the context of international security and disarmament](#)", A/RES/73/32, 2018.
2. UN Secretary-General's High Level Panel on Digital Cooperation, "[The Age of Digital Interdependence](#)", 2019.
3. United Nations Secretary-General, "[Secretary General's High Level Panel on Digital Cooperation](#)", news release, 2018.
4. UNIDIR, "[2019 Innovations Dialogue: Digital Technologies and International Security](#)", 2019.
5. See pages 21 and 22 for the agenda.
6. To watch the fictional scene-setting scenario video by Dawn Thomas, visit bit.ly/UNIDIR-Innovations
7. UNIDIR primers on quantum computing, IoT and DLT are forthcoming.
8. United Nations Secretary-General, "[Securing Our Common Future, an agenda for disarmament](#)," Office for Disarmament Affairs, 2018, p. 51.
9. However, that does not necessarily imply equal rights among all participants as some participants can have more rights as central administrators, while others have limited privileges.
10. Hybrid ledgers combining those properties exist. The way in which participants authenticate and validate transactions is called a consensus mechanism. Various consensus mechanisms exist. Both of these topics go beyond the scope of this report.
11. The term "trust machine" with regard to DLT was introduced in "[The Promise of the Blockchain: The Trust Machine](#)", The Economist, 31 October 2015.
12. International Telecommunication Union, "[Recommendation ITU-T Y.2060 : Overview of the Internet of Things](#)", 2012.
13. For more information on the OODA loop, see Berndt Brehmer, "[The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control](#)", 10th International Command and Control Research and Technology Symposium, 2005.
14. Lydia Kostopoulos, "[The Role of Data in Algorithmic Decision Making](#)," UNIDIR, 2019.
15. United Nations Secretary-General, "[Securing Our Common Future, an agenda for disarmament](#)," Office for Disarmament Affairs, 2018, p. 70.

CONFERENCE AGENDA

9:00 — 9:30

Opening Remarks

Tatiana Valovaya, *Director-General, United Nations Office at Geneva*
Ambassador Pankaj Sharma, *India*
Ambassador Peter Andreas Beerwerth, *Germany*
Brigadier General H.E. Hassan Saleh Al Nisf, *Qatar*

9:30 — 10:20

Digital Innovations and the Global Security Landscape

How will digital technologies transform international security? What are the characteristics of these innovations that make them challenging to consider through an international security, arms control and disarmament lens?

Dawn H. Thomas, *CNA and Cybersecurity Futures 2025 Project*
Lim May-Ann, *Asia Cloud Computing Association*
Kerstin Vignard, *moderator*

10:20 — 10:30

Coffee 'to go' — move to Tech Track Rooms

10:30 — 12:15

Tech Track Break-out Sessions

These interactive sessions will give participants an initial appreciation of the risks and benefits of these innovations. What are they? How do they work? What implications does their development and diffusion have for international security and stability?

- **Track 1: Quantum Computing** (room XXII)
Patrick Towa, IBM Research
Elsa B. Kania, Center for a New American Security
- **Track 2: Distributed Ledger Technologies, including blockchain** (room XVII)
Suzana Maranhão, ITU Focus Group on Application of DLT
Giacomo Persi Paoli, UNIDIR
- **Track 3: Internet of Things** (room XXV)
Jan-Peter Kleinhans, Stiftung Neue Verantwortung
Madeline Carr, PETRAS National Centre of Excellence in Cybersecurity of the IoT

12:15 — 12:20

Return from Tech Tracks

12:20 — 13:00

Fireside Chat: Security Implications of Artificial Intelligence Beyond Weapon Systems

A moderated discussion on how AI and machine learning may impact:

- *prevention and escalation management of cyber conflicts*
- *strategic command and control systems*
- *data analysis for strategic decision-making*

Kobi Leins, *University of Melbourne*
Arun Sukumar, *Observer Research Foundation*
Lydia Kostopoulos, *moderator*

13:00 — 15:00

Lunch Break

CONFERENCE AGENDA

15:00 — 15:15 **Brief report backs from the Tech Tracks — insights and open questions**

15:15 — 16:30 **Digital Innovations for International Security and Disarmament**

This panel will explore current or near-term beneficial applications of digital innovations, through concrete examples and real use cases.

Quentin Ladetto, Armasuisse

Elina Martikka, Finnish Radiation and Nuclear Safety Authority

Benjamin Ang, Nanyang Technological University

Alejandro Hernandez, Organisation for the Prohibition of Chemical Weapons

Giacomo Persi Paoli, *moderator*

16:30 — 16:45 **Coffee Break**

16:45 — 16:55 **Keynote Address**

Izumi Nakamitsu, High Representative for Disarmament Affairs (by VTC)

16:55 — 17:50 **Concluding Discussion: International Security in the Digital Age**

An open moderated discussion on:

- *How can the risks and benefits of digital innovations be better integrated across all disarmament discussions?*
- *How can the participation of technical specialists and other stakeholders —particularly from the private sector and the research community — be better incorporated in security discussions of digital innovations?*

Renata Dwan, *moderator*

17:50 — 18:00 **Closing Remarks**

Renata Dwan, *moderator*

Ambassador Felix Baumann, *Switzerland*

SUGGESTED BACKGROUND READINGS & MATERIALS

QUANTUM COMPUTING

- [IBM Think Academy: How It Works](#): Quantum Computing (short video)
- [The WIRED Guide](#) to Quantum Computing
- “[Quantum computing and defense](#)” in IISS, The Military Balance 2019
- Quantum Computing Is the [Next Big Security Risk](#)
- Inside the High-Stakes Race to [Make Quantum Computers Work](#)

INTERNET OF THINGS

- [IBM Think Academy: How It Works](#): Internet of Things (short video)
- What is the Internet of Things? [WIRED explains](#)
- [Leveraging the Internet of Things](#) for a More Efficient and Effective Military
- Smart City Tech Would [Make Military Bases Safer](#)
- [Internet of Things Meets the Military and Battlefield](#): Connecting Gear and Biometric Wearables for an IoMT and IoBT
- Click Here to Kill Everyone: With the Internet of Things, We’re Building a World-size Robot. [How are We Going to Control It?](#)

DISTRIBUTED LEDGER TECHNOLOGY

- Centre for International Governance Innovations: [What is BLOCKCHAIN?](#) (short video)
- [The WIRED Guide](#) to Blockchain
- The Differences between [Blockchain & Distributed Ledger Technology](#)
- [Better Than a Floppy](#)—The Potential of Distributed Ledger Technology for Nuclear Safeguards Information Management
- Why Military Blockchain is Critical in [the Age of Cyber Warfare](#)
- How the [Blockchain is Redefining Trust](#)
- [Blockchains in National Defense](#): Trustworthy Systems in a Trustless World
- [The Role of Disruptive Technologies in International Security Affairs](#): Making a Case for the Use of Blockchain Tech to Cope with Illicit Arms Trade
- Once Hailed as Unhackable, [Blockchains are Now Getting Hacked](#)

OTHER READINGS ON INTERNATIONAL SECURITY & SCIENTIFIC & TECHNOLOGICAL INNOVATIONS

- UC Berkeley’s Centre for Long-Term Cybersecurity “[Futures](#)” Scenarios
- Defence Future Technologies: [What We See on the Horizon](#)
- Trust Mechanisms and Online Platforms: [A Regulatory Response](#)



VISIT OUR WEBSITE...

for the full list of readings and materials
at bit.ly/UNIDIR-Innovations

ACKNOWLEDGEMENTS

The 2019 Innovations Dialogue was a one-day informal seminar sponsored by the Governments of Germany, India, Qatar and Switzerland. UNIDIR's Security and Technology Programme is supported by Germany, the Netherlands, Norway and Switzerland.

UNIDIR would like to thank Merel Ekelhof, Alisha Anand, Oleg Demidov, Giacomo Persi Paoli, Kerstin Vignard and Lydia Kostopoulos for their contributions to this summary report. Support from Siti Nabila Aisyah, Aaron J. Buckley, and Eric Schulz helped make this report possible.

ABOUT UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

ABOUT THE SECURITY & TECHNOLOGY PROGRAMME

Contemporary developments in science and technology present new opportunities as well as challenges to international security and disarmament. UNIDIR's Security and Technology Programme (SecTec) seeks to build knowledge and awareness on the international security implications and risks of specific technological innovations and convenes stakeholders to explore ideas and develop new thinking on ways to address them.

