Proceedings of the

The Security Challenges of Emerging Technologies

conference

hosted by:

the Centre for International Policy Studies (CIPS)
&
the Canadian Pugwash Group (CPG)

University of Ottawa, 20 October 2023

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
AUKUS	Australian United Kingdom United States
AW	Autonomous Weapons
CTBT	Comprehensive Nuclear-Test-Ban Treaty
EDT	Emerging Disruptive Technology
EU	European Union
IAEA	International Atomic Energy Agency
ICBM	Intercontinental Ballistic Missile
IHL	International Humanitarian Law
ITU	International Telecommunication Union
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
NWC	Nuclear Weapons Convention
NWS	Nuclear Weapon State
PAROS	Prevention of an Arms Race in Space
PPWT	Prevention of the Placement of Weapons in Outer Space
P5	Permanent Members of the United Nation Security Council
REAIM	Responsible Artificial Intelligence in the Military Domain
TPNW	Treaty on the Prohibition of Nuclear Weapons
UAV	Unmanned aerial vehicle

Summary

In an era defined by technological leaps and ground-breaking innovations, the nexus between emerging technologies and national security is a pressing concern. While holding immense promise, emerging technologies present formidable security challenges that demand collective attention and innovative solutions. In this context, the Canadian Pugwash Group (CPG) and the Centre for International Policy Studies (CIPS) at the University of Ottawa held a policy conference entitled “The Security Challenges of Emerging Technologies”.

A set of five expert panels dissected the multifaceted landscape of emerging technologies and security. After a scene-setting address, the first panel considered the ever-evolving dynamics of cyber security, where the offense-defense dynamic continually reshapes the digital battleground. The second panel on AI and autonomous weapons confronted the ethical considerations surrounding the integration of artificial intelligence into autonomous weapon systems, raising crucial questions about responsible innovation and adherence to international humanitarian law. The third panel examined the potential consequences of an arms race in outer space against a backdrop of the exponential growth in satellites and current strains on international cooperation. The fourth panel addressed the ever-present risks associated with nuclear weapons and the risks of strategic instability as arms control “guardrails” are abandoned. The concluding panel took up the question of what contribution Canada could make to ensuring a world where the benefits of emerging technologies are harvested while their threats to international security are contained.

The CPG-CIPS policy conference provided a unique platform for engagement with leading experts, policymakers, researchers and the concerned public, as part of an ongoing discourse on how best to navigate the complex intersection of emerging technologies and security.

Introduction and Scene-setting Address

- Welcome: Alexandra Gheciu
- Speaker: Cesar Jaramillo

Dr. Gheciu and Mr. Jaramillo opened the conference with remarks on three poignant issues, each of which set the stage for the discussions held throughout the day. The first was a note of solidarity, which began with the recognition that CIPS and Pugwash were continuing their friendship and collaborative effort to explore pressing challenges in contemporary international relations. The spirit of solidarity was a thread that weaved together the need for an interdisciplinary approach to the discussions that would follow, but also the need for academics and policy makers to embody a sense of responsibility in putting forth proposals. Taking a responsible approach is a "question of humanity" and crucial in this new era of security. It is in this new era where the world faces new challenges in addition to old ones. The emergence of new technologies compounds older and still unsolved complexities facing the international community. One such complexity is that emergent technologies have multiple dimensions in their potential for both good and harm. Finally, it was noted that Canada is the primary stakeholder in this discussion. Canada has a strong role to play both in these conversations as well as in taking action towards mitigating challenges and proposing solutions. Canada must use its power towards collective security.

Panel 1- "Cyber Security – the Offense-Defence Dynamic"

- Moderator: Nisha Shah
- Speakers: Walter Dorn, Leah West

Dr. Leah West

Dr. West opened her remarks by noting we do not often talk about defensive laws and the obligation that states have to defend their citizens against cyber attacks. Russia's invasion of Ukraine in 2022 began with cyber attacks against Ukrainian cyber infrastructure including its broadband internet service provider and 19 government and critical entities.[1] This type of strategy can prepare ground troops by identifying, degrading, or disrupting key military objectives. Furthermore, cyber attacks present the opportunity to compromise the integrity of infrastructure without physical presence thus reducing risk to people and material, and provides a level of deniability. In advance of these attacks, Ukraine took the effort to ward off cyber attacks by changing its laws on the protection of its public and private data which had long prohibited government from processing and storing data in public clouds. This change permitted Ukraine to migrate civil and military data from physical servers located at Ukraine's borders to, with the assistance of Microsoft[2] and Amazon,[3] private servers across Europe. This highlights not only the ability to quickly move data across borders, but also that commercial interests can advise on

[1] Reuters (2022). "Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say." https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/
[2] Microsoft (2023). "How technology helped Ukraine resist during wartime." https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/
[3] Amazon (2023). "How Amazon is Helping Ukraine." https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine

wartime strategy. This is a new development in contemporary conflict. It is not clear whether this strategy is consistent with international humanitarian law. States have an obligation to defend civilians and civilian objects from cyber attacks. The rules governing the precaution against attack do not simply prohibit conduct but also create positive obligations on states to either segregate civilians, or if segregation is not possible to take other necessary precautions. The literature on how this applies to the cyber context is theoretical. In October 2023 the ICRC made recommendations on mitigating harms to data including segregating military from civilian data.[4] During the Ukraine conflict, however, the exact opposite happened. With the help of Microsoft, civilian data was interspersed with military data, and Ukraine ceased to rely on isolated government infrastructure in favour of civilian networks over which Ukraine has no authority and seemingly no capacity to defend or protect. Ukraine is using private European Union (EU) data infrastructure to shield itself from attack. These strategies are so far effective but whether they are lawful according to the core international humanitarian law (IHL) principle of distinction between military and civilian objects remains unanswered.

Debates in international law focus on two key issues: what counts as a cyber attack, and what is an object? Dr. West states the bigger and unexplored question is in fact what it means for something in cyber space to fall under a state's control? Experts responsible for the Tallinn Manual,[5] the leading text on international law and cyber space, are divided. The majority argue that if an object is on a state's territory it is under a state's control. The minority consider a wider notion of jurisdiction and argue that territory is a necessary but insufficient qualifier. The question remains: what if a state has control over cyber space and the object is not on territory? International law does not stipulate the obligations in this context and is thus underdeveloped. When a state hides its data in private servers in multiple jurisdictions, these objects count as direct military targets. This is the situation we see in Ukraine, whose obligation to protect civilian data ended the moment it interspersed it with its military data. Dr. West ended her comments by encouraging a rethinking of the recommendations designed to protect civilians and whether they are likely to comply with international law. Avoiding thinking through the consequences of conflict and technology and continuing to think in the abstract will contribute to recommendations that will not survive first contact. This can result in an environment where states are more likely to operate in grey zone spaces and where shaping state policy is made more difficult.

Dr. Walter Dorn

Dr. Dorn opened his remarks by noting that an effective strategy to managing cyber security could be through a Global Commons approach, similar to the model used to govern the oceans, and foundational to the UN Convention on the Law of the Sea (UNCLOS). Taking a commons approach to cyber security can help identify gaps in international law and potential solutions; in other words, to bring governance to an ungoverned space. Outer space is an example of a less governed space, but one in which there exists a basic governance framework through the 1967 Outer Space Treaty.[6] In contrast, cyber space is the 'wild west'. Governance of cyber security is driven largely by industry and thus by profit. It is highly unreliable and marked by inefficiency and the potential for malicious parties. The EU is a body that can guide us in this respect. The EU is home to considerable cyber space usage and traffic, and implemented the General Data Protection Regulation[7] in 2019. Dr. Dorn noted that global problems, however, require global solutions. There are a few key groups working on strengthening the governance of cyber security.

[4] See https://www.icrc.org/en/statement-unga78-first-committee-disarmament
[5] The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/research/tallinn-manual/
[6] Formally known as formally Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. See https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
[7] See https://gdpr-info.eu/

Pursuant to the UN General Assembly resolution 73/266,[8] a Group of Governmental Experts on Advancing responsible State behaviour in cyber space in the context of international security was established in 2018. Stakeholders in the field of international humanitarian law and laws of armed conflict have proposed limits on the conduct of cyber operations.[9] The NATO Cooperative Cyber Defence Centre of Excellence was created in 2008 to carry out cyber defence research, training and exercises in the areas of technology, strategy, operations and law.[10] Dr. Dorn claims what is needed is an international convention that can unite the multiple rules and regulations proposed by these various bodies.

There are a few key principles to consider in what such an international approach could entail. The laws of peacekeeping, for example, could apply to the governance of cyber security. The laws mandate evidence based and impartial monitoring of activities on the ground. The laws can provide a framework through which we can ask questions on what conflict means in cyber space, and whether conflict, and hacking, for example, can be monitored. Another element to consider is buffer zones in cyber relations. On the battlefield, buffer zones are neutral pieces of territory between two competing forces. Dr. Dorn observes that it may be possible to implement such zones in cyber space, where cyber layering could separate traffic between two cyber spaces and prevent opportunities for parties to commit intentional border gateway protocol hijacking attacks, such as when China was able to reroute European traffic for two hours in 2019.[11] Dr. Dorn observes that these monitoring and layering principles can find currency with United Nations organizations including the International Telecommunication Union (ITU),[12] and the International Atomic Energy Agency (IAEA)[13] which are proficient in monitoring, for example. There are, however, few Individuals and organizations who can speak on matters of cyber security revealing a significant gap in capacity. Dr. Dorn ended his remarks by reiterating that cyber security is a global challenge, and thus requires global capacity.

Discussion

Dr. Shah opened the discussion by observing that several conceptual and empirical questions emerge concerning the nature of a civilian object, the material structure of the theatre of operations, what the global commons comprise, and about who has authority in these contexts. A question was posed concerning whether there has there been an evolution in the thinking in cyber operations vis-à-vis the use of force. It was responded that states have started to articulate how they view the law. Canada in May 2022, for example, released a statement on how international law applies to cyber space including on the use of force.[14] If the effects of the act give rise to what we would see in the physical space, the act is considered a use of force. The prior question is what constitutes a violation of sovereignty in cyber space? States are committing acts that violate targets, but these are not considered violations of sovereignty; cyber attacks are not considered violations in the same way as attacking a physical weapons storage facility, for example. Relatedly, assessing the proportionality of a cyber or kinetic attack in the context of escalation depends on what is lost in civilian vis-à-vis military objects. It was noted that definitions can be unclear. For example, what are civil actors and what are government actors, and what is considered a letter of mark? How does one identify a civilian target vis-à-vis an

[8] https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F266&Language=E&DeviceType=Desktop&LangRequested=False
[9] See https://www.icrc.org/en/document/international-humanitarian-law-limits-cyber-operations
[10] The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/
[11] Security Affairs (2019). "Recently a large chunk of European mobile traffic was rerouted through China Telecom." https://securityaffairs.com/86808/security/china-telecom-traffic-hijacking.html
[12] https://www.itu.int/en/Pages/default.aspx
[13] https://www.iaea.org/
[14] See https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

object of attack, for example a hospital which could be private or public but which houses civilians? It was responded that it depends on whether civilian acts aim to achieve military objectives. It is now easier for civilians to participate in hostilities. We see this in civilian hackers and the Ukrainian application that asks civilians to take photos of Russian armament and upload this to the Ukrainian government. Furthermore, we only have legal opinions when what is needed is jurisprudence that takes into consideration *mens rea*. This underscores the need for broad international machinery to regulate participation.

The clamour to participate in military actions from industry and private actors encourages us to ask what commercial operators should know with respect to their civilian employees participating in armed conflict. It was responded that the ICRC made recent recommendations to states and technology companies that data should be segregated, but companies must acknowledge that their employees can become targetable. This is yet another reason for the creation of a separate set of rules that applies beyond the context of IHL. It was asked how we can address attribution in the age of deniability. It was responded that this is difficult as there are mechanisms designed to keep actions private including through encryption, the Dark Web, and TORs, for example. It is not impossible, however, and positive examples include trend-spotting where consistent actions or repeated patters become visible. A concern was put forth on whether there exists a Plan B when it comes to protecting data that is increasingly agile. IHL is the best provisional regime we have, but it is important to acknowledge that states are hedging their positions vis-à-vis the rapid evolution of technology. It was asked whether IHL is sufficient to rise to these challenges. On one hand, it is risky to say that IHL is insufficient because this may encourage stakeholders to discontinue thinking about ways IHL could be deployed in the context of evolving technology and in an environment where states are reticent to come to the table. On the other hand, IHL is insufficient in the sense that it has very few outright prohibitions; it is always a question of proportionality. There are other treaties that ban certain weapons in all potential circumstances because of their harmful implications; these are useful because their objective is to protect civilians, which is not the primary concern IHL. How, then, can the normative framework for states be enhanced and state compliance be encouraged? It was responded that we need new rules on the prevention of cyber attacks: our norms are insufficient. We need a treaty with binding mechanisms. There is room for inspiration, but we need customisation and international authority with keys to enter national spaces to inspect and enforce.

Panelists were asked about the strategy of so-called good actors using viruses to attack the critical infrastructure of so-called bad actors, an example of which is Stuxnet.[15] It was responded that because Stuxnet was not considered an armed conflict, the laws of war did not apply. This is a salient example of the need for a regulatory framework that would apply to all states. The Oxford Process developed in 2020[16] may be a good basis for guidance in this respect. It was asked whether the prohibitions on land mines, chemical weapons, and cluster munitions, all of which consider unintended consequences on civilians, could be a basis for a treaty on cyber security. It was responded that yes, inspiration could come from arms control treaties, but cyber space's dual use capability means that rather than an object or tool, cyber space is a domain in an addition to land, sea, and air. Thus a broader approach is needed.

[15] IEEE Spectrum (2013). "The Real Story of Stuxnet." https://spectrum.ieee.org/the-real-story-of-stuxnet

[16] The Oxford Process on International Law Protections in Cyberspace. https://www.elac.ox.ac.uk/the-oxford-process/

Panel 2 - "Artificial Intelligence and Autonomous Weapon Systems"

- Moderator: Cesar Jaramillo
- Speakers: Branka Marijan, Srdjan Vucetic

Dr. Branka Marijan

Dr. Marijan opened her discussion by noting that AI in military uses is evolving quickly and has a broad application. The primary concern is the use of AI that enables autonomy in weapons systems, and the capacity AI holds to change the information environment in which war takes place. We have moved from hypothetical uses to real time applications on the battlefield. Examples include facial recognition technology in Ukraine that is used to identify the deceased but also individuals who are potential war criminals.[17] Another is the Saker Scout Drone a quad-copter integrated with AI and the Delta Intelligence Distribution System which gathers information on the battlefield, including military objects, and relays that information to human operators.[18] The first use of AI weapons was noted, but unconfirmed, in a 2021 United Nations report[19] that claimed a Turkish Kargu 2 Drone[20] was used against **r**etreating forces in Libya. This example highlights the importance of language around the use of such tools, as the manufacturer claimed the Kargu 2 drone had autonomous capabilities yet Turkish officials claimed the tool was not fully autonomous but semi-autonomous. Industry has an interest to promote their tools as autonomous yet states have incentive to remain within the limits of acceptable norms. Advancements in this field are furthered by competition between states. The speed and efficiency of response is of great appeal to militaries. For example, it can take an AI tool 20 minutes to analyse data that could take a human analyst 100 hours to complete. The military space is welcoming AI advancements in the civilian space, and there is less separation between the two. Industry is willing to test products in active conflict zones, two examples of which are Microsoft and Palantir.[21] Technological power still remains within a few powerful states and a few powerful actors within those states, but non-state actors can access important technologies like drones. Inherently a dual use tool, AI is open source, and its code is publicised.

We do not currently have a framework for autonomous weapons systems as these developments are taking place on the battlefield. Dr. Marijan noted several opportunities for governance in this area and some challenges with implementation. The Convention on Certain Conventional Weapons (CCCW) is an important incubator to helps us understand these issues, and since 2014 has been concerned with autonomous weapons. The CCCW has become a stalled forum in part because of its consensus model which permits vetoing. What we are seeing is a push for new mechanisms and new regulations. For example, Austria tabled a resolution[22] at the First Committee at the UNGA in October 2023[23] to develop a new type of forum for these issues. Regional moves are also taking place. Costa Rica is leading a call from Caribbean and Latin American states for the prohibition of

[17] Reuters (2022). "Exclusive: Ukraine has started using Clearview AI's facial recognition during war." https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/
[18] Forbes (2023). "Ukraine's AI Drones Seek And Attack Russian Forces Without Human Oversight." https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/?sh=6d55b93466da
[19] NY Times (2021). "A.I. Drone May Have Acted on Its Own in Attacking Fighters, U.N. Says." https://www.nytimes.com/2021/06/03/world/africa/libya-drone.html
[20] Liebers Institute West Point (2021). "The Kargu-2 Autonomous Attack Drone: Legal & Ethical Dimensions." https://lieber.westpoint.edu/kargu-2-autonomous-attack-drone-legal-ethical/
[21] Tech Informed (2023). "One year on: 10 technologies used in the war in Ukraine." https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/
[22] See https://automatedresearch.org/news/state_position/austria/
[23] See https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-eighth-session-2023

autonomous weapons.[24] The U.S.A. would like to see a political declaration. As a result, we now have parallel processes, which may have advantages. We need more creative thinking on these issues outside these arenas, and we also need a comprehensive understanding of the technology that is evolving, transforming and proliferating, and which is advancing beyond our regulatory frameworks.

A related conversation is taking place on the responsible military use of AI. The Netherlands and the Republic of Korea hosted the first global Summit on Responsible Artificial Intelligence in the Military Domain (REAIM) in 2023,[25] and the next will take place in South Korea in 2024, but this conversation is fizzling out. On these issues, actors are good at talking to allies but not good at talking to adversaries. What we need is a multilateral forum on regulation and prohibition in the context of affecting civilians. The level of nuance and policy development is insufficient, and what is happening on the battlefield today is already undermining IHL. IHL is insufficient to answer questions regarding accountability. Dr. Marijan asked who is accountable if a system makes a mistake, if it targets civilians? Can we certify systems to ensure they are safe for use? Should they be making decisions regarding human lives? These are questions of intent and ethics which we have not yet asked, yet we are deploying these autonomous weapons. The issue of autonomous weapons is not a futuristic notion based on science fiction but happening today and may fall by the wayside because of the perception that we have the time to address it.

Dr. Srdjan Vucetic

Dr. Vucetic's discussion approached the issue of AI and weapons around three questions: What is the political economy of AI? What is Canada's role in this, if any? Which power blocs stand to emerge victorious in the AI race? Dr. Vucetic noted that the answer to the first question is unknown. There are at least two reasons for this: there is scarce data on the topic, and the notion of the 'defence industry' is a misnomer. Dr. Vucetic explained that there is no single AI defence industry, though there is an effort to categorise a broad spectrum of characteristics of such. For example, AI is a dual use tool that can be deployed in both military and non-military settings. It is significant and akin to other large scale technological developments in history such as the steamship and the telegraph. AI is highly commodified and ubiquitous and there is substantial investment in this emerging industry. Furthermore, whereas a prominent narrative in media is concerned with the so-called "big shinies", the larger military capabilities in submarines and planes, it is more difficult to capture AI in the context of small or light arms as drones and UAVs, for example, vary in size. In considering Canada's role in this, Dr. Vucetic noted that Canada, like most smaller powers, is debating these basic issues. A key question for Canada concerns the right balance between governments who are both regulators and consumers of military AI technology. But the answers are not easy in any context. Dr. Vucetic noted that AI is emergent in strategic thinking and while it can be both forbidding and obscure, it is also a factor in 'boosterism', where strategy is well thought through in terms of which side is emerging victorious in a particular conflict. Of concern in this respect is the geostrategic China-U.S.A. contest. In the context of AI, the U.S.A. has at least five advantages. First, the Englishization of the world means that the U.S.A. holds a sustainable competitive advantage in the areas of research and development, seen in its ability to recruit top global talent. Second, the U.S.A. is near-autarkic in its defence procurement, and third, has achieved economy of scale in this area. Fourth, it has robust industrial and integrational capacity to produce AI tools and has a 'first mover advantage' in AI platforms enjoying network effects with private industry. Finally, the U.S.A. is able to leverage its experience on the battlefield as a data source in the development of AI weapons. Importantly, this leverage includes battlefield experience of U.S. allies, too

[24] Human Rights Watch (2023). "Latin America and Caribbean Nations Rally Against Autonomous Weapons Systems." https://www.hrw.org/news/2023/03/06/latin-america-and-caribbean-nations-rally-against-autonomous-weapons-systems

[25] See https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/reaim/about-reaim-2023

-- Ukraine and Israel, for example. Dr. Vucetic noted that China is trying to match these advantages and differs from the U.S.A. in its approach to development, production, procurement and more. For example, China applies a top down approach by using centralised guidance funds to select private companies for AI development, whereas the U.S.A. uses a bottom-up strategy and receives AI opportunities from industry. A key lesson here is that the outcome of the AI contest will be decisive for the future as AI-powered weapons and fighting can negate U.S.A. military advantages. Ending on a note of optimism, Dr. Vucetic noted that despite competition, great powers can find ways to coexist to avoid mutual destruction. China and the U.S.A. depend on each other for solutions to climate change, for example, among other pressing challenges.

Discussion

Panelists were asked to respond to the observation that norms must catch up with reality, but in the context of AI, the gap is increasing because of the rapidity with which technology is evolving. It was responded that we should be thinking about platforms, and the fact that any platform can be adapted with networking and autonomous capabilities. Platforms do not need to be sophisticated, and the important questions concern what autonomy is, and what is permissible in this context. A question was posed on Canada's role, to which it was responded that Canada is preparing updates on defence policy and on AI and responsible military. The government gave the previous Minister of Foreign Affairs Champagne the mandate to support international efforts to negotiate a treaty that would prohibit fully autonomous weapons, but this direction was not acted upon in any meaningful way, and the reference to this mandate has been removed from subsequent mandate letters. We are told that Canada is functioning under the belief that it still applies, because there is no clear direction that it no longer applies. A question was posed on the roles of civil society and states concerning autonomous weapons. It was responded that despite smaller states acting as champions, the CCCW forum is dominated by Russia. Canada has acknowledged that the CCCW is but one appropriate forum. This is a small but major advancement. Canada appears to be in the 'wait and see' camp but middle powers, including Canada, need to engage more strongly to overcome gridlock in this area.

A question was posed regarding the fact that AI software is open-source, thus posing the same challenges to all states, including to China. It was responded that the U.S.A. CHIPS and Science Act,[26] for example, is an effort to recognise that open-source and software are important but there is also a need to address China's production of kinds of technologies beyond data science, advance computing, and autonomous systems. It is also necessary to look at the so-called second tier producers and traders such as Turkey and South Korea where there are clear advantages of the open-source world used to create industries that can compete in some niche ways with larger exporters of the P5 countries. Furthermore, states can exert influence on the chip market to control exports. Who has computing power, who has the most advanced chips, and the fact that humans are still needed to repair hardware, are still concrete elements of this discussion. Furthermore, China is not just thinking about how to disrupt adversary advantages, for example how to produce a system that can attack an entire satellite system, but also creating new technologies that are difficult to identify.

Given that China has committed to not using AI but has stipulated that it will continue developing these tools, how can we think about China's approach to working within the international system in this context? It was responded that China is savvy in this respect and uses ambiguous language to participate in international institutional mechanisms. China has supported prohibition on offensive use of autonomous weapons, but not on the use of defensive weapons. This is important as there is a fine line between what is considered offensive and defensive. China did not offer clarity on

[26] See https://www.commerce.gov/news/press-releases/2023/09/biden-harris-administration-announces-chips-america-funding-opportunity

this matter and other countries did not push for this. We must encourage more diplomacy and not fall into self-fulling prophecy on China the amplification of its civil military fusion. It was then asked how this relates to Canada and universities. For example, Canada partners with Chinese universities and the Chine military, but Canada says this will no longer be tolerated when it comes to public funding. This leaves out, however, civilians who are sometimes required to work with the Chinese military. China is also no longer publicising its technological research relevant to military uses. It was noted that many countries partner with China in its Belt Road Initiative to use Chinese technology including surveillance, policing, and training on using AI for censorship.

It was asked whether humans, data, or algorithms have the advantage in this context. In the context of human talent, the U.S.A. has the advantage due to its liberal approach of encouraging human capital. Canada is among the top five countries for AI talent, but these advantages are not infinite, as the best people are recruited by the best companies, and these are in the U.S.A. Canada is good at research and ethics but scores poorly in scaling defensive interest and holds a disadvantage for future defence applications. For example, Canada had little to offer in response to the September 15 2021 AUKUS announcement,[27] specifically Pillar 2 which is to enhance joint capabilities and interoperability amongst these states.[28] Canada is ill-equipped to participate in dialogue as recruitment and training are insufficient and do not match other states' efforts.

A final question concerned what is needed to improve global governance on this issue and keep up with the pace of change. Responses noted the need to enhance state capacity, included addressing increasing industry lobbying, and adaption of military technology for smaller components in the so-called military retail complex. We also need to update regulations on expert control. We also need a political vision from Canada; Canada needs to not only be present as a member of an alliance, but also determine and then pose questions driven by our strategic considerations. Canada also needs to publish a national strategy and defence policy that address other related elements including recruitment and retention, climate change disaster, and defence procurement. The Q and A period was closed with the reflections that heightened vulnerability may outweigh perceived benefits of AI and autonomous weapons, and that arms control architecture may serve to guide progress on defining what a weapon is.

Panel 3 - "The Arms Race in Outer Space – Prevention or Proliferation?"

- Moderator: Habib Massoud
- Speakers: Jessica West, Paul Meyer

Paul Meyer

Mr. Meyer began his remarks by noting several inherent challenges concerning weapons and the realm of outer space. Mr. Meyer stressed the importance of outer space for global well-being and security, and the need to keep operations in space free from threats from states or non-state actors. There has been an exponential growth in satellites in various orbits upon which global society is increasingly dependent. It is difficult to determine reliable statistics on how many and what type of satellites are currently in orbit. Databases are frequently updated with rising figures and it is difficult at times to distinguish between active and defunct satellites. Furthermore, the governance of outer space is a paradox as despite the growing role of the private sector it remains within the purview of states. This

[27] See https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/
[28] See https://www.csis.org/analysis/aukus-pillar-two-advancing-capabilities-united-states-united-kingdom-and-australia

means it is also subject to the vagaries of inter-state relations. Despite the need for cooperation amongst states to ensure the safe and secure utilization of outer space, the current situation is fraught with tension and mistrust. The effort to prevent an arms race in space has been led by the United Nations. The 1967 Outer Space Treaty[29] provided common ground in calling for the peaceful uses and non-national appropriation of outer space including prohibiting the stationing of weapons of mass destruction in orbit. Several measures were put forth in the 1960s and 1970s, and more recently Russia and China have proposed a Treaty on the Prevention of Placement of Weapons in Outer Space (PPWT.

Mr. Meyer noted key tensions in the struggle to prevent the weaponization of space. Despite states upholding the call to prevent an arms race in space, there is scant effort to carry this out in practice. There is significant divergence amongst states as to what is the most effective approach. For example, China, Russia, and Indonesia favour legally binding agreements and argue that only treaties with the force of law will have staying power for compliance. Other states (U.S.A and allies) tend to favour politically binding measures, for example, those that mandate transparency and confidence building measures amongst parties. Adding to this is the development of counter space capabilities including anti-satellite weapons (ASATs), which are tested and launched into orbit causing a debris field that can linger for decades. Such debris is non-discriminatory and threatens the safe operation of spacecraft irrespective of state ownership. These facts demonstrate that we are experiencing an arms race precisely when restraint is needed.

Mr. Meyer pointed to a renewed effort towards space security. Amidst an admittedly hostile diplomatic environment, the United Nations, pursuant to General Assembly resolution 76/231,[30] established the Open-Ended Working Group on reducing space threats through norms, rules and principles of responsible behaviours. The working group met four times in 2022-2023 but failed to produce a report on substance or even a procedural report. Resolutions were adopted at the UN General Assembly's First Committee in October 2023 that supported establishing two follow up working groups. Mr. Meyer saw some merit in this otherwise duplicative effort as it would allow discussion of both the political and the legal approaches. This may overcome the existing stalemate over where the focus of negotiations under UN auspices should be. There should be scope for both developing transparency and confidence building measures and elaborating a legally binding instrument that would reinforce the existing legal regime represented by the Outer Space Treaty.

Dr. Jessica West

Dr. West opened her remarks by making the claim that it is no longer clear if space has been weaponized or not and outlined several reasons why. While there have been many elaborate proposals for weapons systems in space over the years, most of which have failed because of physics and costs, advancements in technology are making some concepts more feasible. We have already seen kinetic ground-based weapons tested to destroy objects in space. Other non-kinetic capabilities, including cyber, have been used to target satellites from earth; while we do not know if such capabilities are embedded in orbital payload, Dr. West suspects that there are satellite jammers[31] in orbit. Echoing comments by Dr. Marijan's remarks on the blurred distinction between civilian and military applications of technology, Dr. West noted that dual purpose capabilities in space such as advanced robotics and manoeuverability make it difficult to know if they are deployed for benign or harmful applications, or

[29] Formally known as formally Treaty on the Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies. See https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
[30] See https://undocs.org/Home/Mobile?FinalSymbol=a%2Fres%2F76%2F231&Language=E&DeviceType=Desktop&LangRequested=False
[31] On the Radar (2019). "Satellite Jamming." https://ontheradar.csis.org/issue-briefs/satellite-jamming/

both. China recently used one of its own satellites to grab another.[32] Such capabilities can aid efforts to reduce space debris and service satellites, but they can also be used to harm satellites.

The prospect that weapons may have been deployed in outer space is not new. During the Cold War, the Soviet Union orbited a fractional orbital bombardment system capable of delivering nuclear weapons through space. although ostensibly a violation of the Outer Space Treaty, objections were not raised at the time because the system was not tested or used for this purpose. Nonetheless, the capability was in orbit for approximately a decade. Today, there are accusations that China is developing a similar capability to deliver hypersonic glide vehicles from orbit, targeting Earth. Space planes are another capability that have murky applications and intentions. It is thus not a question of whether outer space has been weaponised, but how, and how do we know. Instead of a norm of non-weaponization of space, we have developed one of not talking about weapons in space; this norm of silence has been productive for the potential of weaponization of space and for its accelerated militarization.

Dr. West attributes this norm of silence to what she called the "myth of peace in outer space." Drawing on the argument made by Dr. Bleddyn Bowen in his latest book "Original Sin"[33] that points to the fact that the first satellite launched was a military one as a key source of insecurity in outer space today, Dr. West counters that the greater sin is the narrative that this launch was a peaceful endeavour. We live in a fog of peace in outer space where we uphold this narrative to mask and justify the potential harms of military capabilities under a 'peaceful discourse'. For example, the release of projectiles from a Russian satellite was labelled as a satellite servicing experiment. Other elements of this narrative include a growing focus on "defensive capabilities" in outer space, which range from lasers and jammers to possible kinetic capabilities. A growing range of commercial capabilities and activities adds yet another layer of uncertainty. This fog of peace makes it difficult to see, understand and point out non-peaceful actions in outer space. This is dangerous as it blurs the distinction between what peace does and does not look like in outer space. It also impedes arms control: we cannot govern what we do not acknowledge exists.

Dr. West ended her remarks by noting challenges to this norm of silence in outer space, including the recently concluded United Nations Open-Ended Working Group on Reducing Space Threats, which has received a second mandate. Yet there remains strong reticence to define what a space weapon is, which remains a persistent obstacle to arms control in space. This obstacle is made greater by the lack of trust among states that is amplified by dual-purpose technology. For example, there is suspicion of efforts to ban weapons in space by states that are simultaneously deploying capabilities in orbit that could be used as such. The difficulty in defining space weapons also makes possible verification of such capabilities challenging.

The upside is that many states without significant military space capabilities increasingly see themselves as stakeholders and are bringing renewed energy to space diplomacy. However, there is a risk that this engagement may wane or splinter in face of competing diplomatic initiatives at the UN. However, in the cyber security context a similar twin approach involving both a UN Group of Government Experts and an Open Ended Working Group, has been able to find some success, which provides a glimmer of optimism for outer space.

Discussion

Mr. Massoud opened the discussion period by asking whether drafting a new treaty concerning the weaponisation of space is a viable option. It was responded that states are wary about constraining

[32] DW (2023). "China building ability to hijack enemy satellites: report." https://www.dw.com/en/china-building-ability-to-hijack-enemy-satellites-report/a-65392829

[33] See https://global.oup.com/academic/product/original-sin-9780197677315?cc=ca&lang=en&

themselves from future options, and the narrative of self-defence will continue. Therefore, perhaps the question should change from what is a weapon to what does peace look like? Changing the discussion in this way would prompt transparency and accountability for state activities and help to draw distinctions between those that are helpful and those that are harmful. Importantly, we need to better define peace in outer space. We have let the definition of peace remain unclear and grow ever wider, thus possibly encompassing even weapons related activities. Here, a focus on state behaviour can help. But to be successful, initiatives must be inclusive. Previous 'hub and spoke' approaches such as the effort by the European Union to lead development of a Code of Conduct for Space Activities led to a sentiment that non-EU interests were not considered equitably. Furthermore, China and Russia drafted the Prevention of the Placement of Weapons and Threat or use of Force in Outer Space (PPWT) but it remains locked within the non-universal Conference of Disarmament.[34]

A comment was made on the increasing blurriness of authority between civilian and military actors, and the fact that civilians including non-elected entrepreneurs can make decisions related to the battlefield. A prominent example is Elon Musk's restriction of Ukraine's use of the Starlink satellite.[35] It was responded that a resulting security risk is the targeting of commercial satellites that participate in or otherwise aid warfighting activities on Earth. This issue has been raised at the Open-Ended Working Group, specifically Russia has declared that it will retaliate against and target commercial operators that provide Ukraine with space-based imagery and broadband, for example. This raises questions about how to distinguish and protect other civilian users of such systems, which may be linked to critical infrastructure. From the IHL perspective, some have suggested a segregation between civilian and military space systems, but this is impractical. Additional transparency measures are necessary. For example, the Registration Convention requires states that launch a satellite to register with the UN Office for Outer Space Affairs.[36] Although some satellites are now being registered as being military in nature, details about their uses and capabilities remain lacking. Other governance challenges raised by this issue of commercial capabilities and harmful interference include the blurring of space and cyberspace, which are each developing distinct norms of behaviour.

Another comment from the floor noted that perhaps it is time for states to be more forthcoming about their activities – including harmful capabilities – in outer space. Would this make governance efforts more effective? An example of this took place in the nuclear context: once states admitted that they were developing nuclear weapons, greater controls and transparency measures were developed. It was responded that this strategy is referred to as the 'operational approach'. Yet this has the potential for backfiring as some states refuse to admit their militarized space activities which then reinforces the peaceful uses narrative. Yet a key reason for success in the nuclear context was the bilateral nature of negotiations; today states no longer communicate through direct challenges but are instead raising issues and accusations in an increasingly public and politicized way, such as through X and diplomatic notes.

The comment was also made that there is law in outer space for some of these challenges, but that states are loathe to invoke it. For example, when China in 2007 launched its ASAT resulting in thousands of pieces of space debris,[37] few states invoked the Outer Space Treaty and adhered to their obligation to consult other states. International law is weakened in this respect. A final question was posed concerning planetary defence and the risk that the moon could be used as a defensive post from

[34] Reaching Critical Will (no date). "Russia and China table new draft treaty to prevent weapons in space." https://www.reachingcriticalwill.org/disarmament-fora/cd/2014/cd-reports/8908-russia-and-china-table-new-draft-treaty-to-prevent-weapons-in-space

[35] The Guardian (2023). "Fury in Ukraine as Elon Musk's SpaceX limits Starlink use for drones." https://www.theguardian.com/world/2023/feb/09/zelenskiy-aide-takes-aim-at-curbs-on-ukraine-use-of-starlink-to-pilot-drones-elon-musk

[36] See https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/registration-convention.html

[37] Council on Foreign Relations (2007). "China's Anti-Satellite Test." https://www.cfr.org/backgrounder/chinas-anti-satellite-test

which existential threats could be launched. It was responded that the planetary defence is a positive story of international scientific collaboration.

Panel 4 - "Nuclear Weapons and the Risks of Strategic Instability"

- Moderator: Alexandra Gheciu
- Speakers: Tariq Rauf, Peggy Mason

Peggy Mason

Ms. Mason outlined the role of AI in nuclear command systems and noted that AI integration is being used to improve the capabilities of early-warning and surveillance systems, to comb through large data sets, make predictions about enemy behaviour, enhance protection against cyberattacks, and improve communications infrastructure throughout nuclear command systems.[38] This support for AI integration is taking place at the same time as a modernization of the command apparatus of all nine nuclear-armed states.[39] Factors influencing states to fully automate their nuclear systems include the appeal for smaller nuclear weapons states (NWS) to hold an effective first-strike deterrent, and the response of leading nuclear powers to new hypersonic delivery systems[40] that can bypass early warning altogether.

Ms. Mason noted that in February 2023, the U.S. Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy[41] outlined a particularly important 'best practice' concerning nuclear weapons: "States should maintain human control and involvement for all actions critical to informing and executing sovereign decisions concerning nuclear weapons employment." This requires that "appropriate levels of human judgment" be applied (as opposed to the much more rigorous "meaningful human control" called for by many[42]) but "appropriate" means that the appropriate level of human judgment or control can mean none at all. The U.S. Declaration avoids this challenge as it requires the maintenance of human control and involvement for all actions critical to nuclear arms and AI. Drawing from comments made by Peter Rautenberg,[43] Ms. Mason noted that maintaining human involvement may not be sufficient where AI and nuclear weapons are concerned, and that relying on this safeguard could result in a hidden increase of risk, outlined as follows:

- The sheer volume of code required in AI systems used for nuclear command and control makes errors and technical challenges inevitable.
- AI systems program themselves in ways that make them innately opaque to humans.
- AI systems are "brittle" and could break down when in unfamiliar territory for which they were not trained.
- AI systems will take on human biases in the training process.[44]

[38] See The Stockholm International Peace Research Institute (2020). "Artificial Intelligence, Strategic Stability and Risk." https://www.sipri.org/publications/2020/policy-reports/artificial-intelligence-strategic-stability-and-nuclear-risk
[39] See https://www.armscontrol.org/factsheets/USNuclearModernization
[40] War on the Rocks (2021). "China's Hypersonic Weapons Tests Don't Have to Be a Sputnik Moment." https://warontherocks.com/2021/10/chinas-hypersonic-missile-tests-dont-have-to-be-a-sputnik-moment/
[41] See https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/
[42] For example, by the campaign to Stop Killer Robots. See https://www.stopkillerrobots.org/
[43] Bulletin of the Atomic Scientists (2023). "Keeping humans in the loop is not enough to make AI safe for nuclear weapons." https://thebulletin.org/2023/02/keeping-humans-in-the-loop-is-not-enough-to-make-ai-safe-for-nuclear-weapons/
[44] Ibid.

- Integrating AI into nuclear weapons command systems also affects the humans involved in ways that make them prone to automation bias, where humans become overly reliant on AI and unconsciously assume that the system is correct.[45]
- Military AI designed to rapidly act on advantages could miss de-escalatory opportunities or function too fast for human decision makers to intervene and signal their de-escalatory intent.[46]
- To fully take advantage of machine speed, states could purposefully remove humans from the loop at key junctions.[47]

These growing risks relating to AI and nuclear weapons are taking place against a backdrop of steadily rising tensions between U.S.A. and China. Efforts by the United States to maintain military dominance in Asia through offensive strategies of containment and control are unlikely to succeed, could prove financially unsustainable, and could also backfire by exacerbating the risk of crises, conflict, and rapid escalation in a war.[48] This undermines the type of cooperative efforts needed to agree on effective regulation of AI and nuclear weapons including "changes to nuclear doctrine, policy, and training—alongside workable technical solutions and heavy vetting."[49]

Ms. Mason observed that cooperative efforts are still possible and taking place. The first global Summit on Responsible Artificial Intelligence in the Military Domain (REAIM) in 2023[50] included four of the five declared NWS and 55 other countries whereby the states:

- Underlined the need to put the responsible use of AI higher on the political agenda and to further promote initiatives that make a contribution in this respect;
- Issued a Joint Call to Action on the responsible development, deployment and use of artificial intelligence (AI) in the military domain; and
- Announced that a Global Commission on AI is to be established to raise all-round awareness, clarify how to define AI in the military domain and determine how this technology can be developed, manufactured and deployed responsibly. The Commission will also set out the conditions for the effective governance of AI.

Furthermore, UN Secretary-General António Guterres called for a new global entity,[51] equivalent to the Intergovernmental Panel on Climate Change (IPCC), that could provide information and expertise for member states [and the media] on the science of artificial intelligence. He has appointed a High-Level Panel to report to him by the end of 2023 on AI and its implications. Drawing from the fundamental awareness-raising role that the IPCC has played on climate change, such an entity could effectively galvanize global action on AI regulation in relation to nuclear weapons. Furthermore, such an entity could speak over the nuclear weapons and armaments lobby which has strong influence on the U.S.A. Congress, think tanks and media. Ms. Mason ended her remarks by reiterating that effective AI regulation in relation to nuclear weapons is increasingly hostage to hostile U.S.A. – China relations.

---

[45] The Stockholm International Peace Research Institute (2020). "Artificial Intelligence, Strategic Stability and Risk." https://www.sipri.org/publications/2020/policy-reports/artificial-intelligence-strategic-stability-and-nuclear-risk

[46] Rand Corporation (no date). "Deterrence in the Age of Thinking Machines." https://www.rand.org/pubs/research_reports/RR2797.html

[47] Bulletin of the Atomic Scientists (2023). "Keeping humans in the loop is not enough to make AI safe for nuclear weapons." https://thebulletin.org/2023/02/keeping-humans-in-the-loop-is-not-enough-to-make-ai-safe-for-nuclear-weapons/

[48] Quincy Institute for Responsible Statecraft (2022). "Active Denial: A Roadmap to a More Effective, Stabilizing and Sustainable U.S. Defense Strategy in Asia" https://quincyinst.org/report/active-denial-a-roadmap-to-a-more-effective-stabilizing-and-sustainable-u-s-defense-strategy-in-asia/

[49] Bulletin of the Atomic Scientists (2023). "Keeping humans in the loop is not enough to make AI safe for nuclear weapons." https://thebulletin.org/2023/02/keeping-humans-in-the-loop-is-not-enough-to-make-ai-safe-for-nuclear-weapons/

[50] See https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/reaim/about-reaim-2023

[51] See https://www.un.org/sg/en/content/sg/statement/2023-09-19/secretary-generals-address-the-general-assembly

Rethinking our approach to the governance of AI and nuclear weapons is urgently needed so that strategic dialogue between the U.S.A. and China can begin.

Tariq Rauf

Mr. Rauf remarks focused on the broader issue of strategic stability and emerging disruptive technology (EDT), of which AI is one. He opened with two examples of the so-called 'dead hand system'.[52] During the Cold War, the Soviets were concerned with a U.S.A. first strike, and thus developed a back up compensatory measure that, in the event that Moscow was attacked, would automatically launch an interrogator missile fleet that would fly over the surviving intercontinental ballistic missile (ICBM) silos and then initiate an attack on the U.S.A. This 'dead hand' strategy has been adopted by North Korea in response to South Korea's 'decapitation scenario'[53] capabilities. Mr. Rauf noted that the concept of strategic stability in the area of nuclear weapons has evolved. During the Cold War, the United States and the Soviet Union converged on the concept of strategic stability as a useful construct to manage great power strategic competition and avoid nuclear war. The concept of strategic stability was originally used as a guidance to avoid nuclear or central strategic war by ensuring that both sides had the ability to respond in case the adversary attempted a disarming first strike. Known initially as *first-strike stability* - the need to increase the survivability of nuclear forces and their support structures, - interpretations of the term evolved into the broader *crisis stability*, focused on reducing escalatory pressures in a conflict referring to the lack of incentives to use any form of military power first in a crisis. Finally, *arms race stability* meant that neither side could improve their position relative to the other side by simply building up nuclear forces. Pursuing these goals simultaneously set clear limits to the strategic competition in the Cold War, put a cap on the most destabilizing capabilities, led to actual force reductions and created crisis management tools designed to avoid unintended escalation based on miscalculation and misunderstandings. Cold War-era bilateral arms control negotiations between the U.S.A. and the Soviet Union focused primarily on capabilities that affected strategic stability and resulted in several treaties limiting nuclear weapons and missile defence capabilities. These agreements enhanced first-strike stability by eliminating incentives for a disarming first strike by shaping the structure of forces and limiting the capabilities that increased relative vulnerabilities. Crisis stability was reinforced by reducing the urgency to pre-empt and the likelihood of strategic surprise and miscalculations through increased transparency and predictability, and by establishing lines of communication and conflict-resolution mechanisms. Arms control also enhanced arms race stability by placing qualitative and quantitative limits on certain capabilities to avoid action-reaction military buildups and reduce the likelihood of achieving military dominance by either side.

In the current multilateral and multidomain environment, nuclear security architecture is more complex and the concept of strategic stability has been extended both horizontally and vertically. Horizontally, the bilateral logic of the Cold War is no longer applicable due to China's rise in power. China remains skeptical about using Cold War concepts and claims that a strategic stability relationship only makes sense among nuclear equals, thus it demands U.S.A. recognition of mutual vulnerability. China believes that arms control and U.S.A. engagement efforts are primarily aimed at constraining adversaries, capping China's military modernization, and locking in its vulnerabilities. China argues that because the U.S.A. and Russia possess over 90% of global nuclear forces, it is primarily their responsibility to continue the arms control process bilaterally. China claims that the U.S.A. is the power that generates instability in the Asia-Pacific region, making it responsible to implement greater

[52] See https://www.pulitzer.org/winners/david-e-hoffman

[53] Carnegie Endowment for International Peace (2022). "South Korea's "Decapitation" Strategy Against North Korea Has More Risks Than Benefits." https://carnegieendowment.org/2022/08/15/south-korea-s-decapitation-strategy-against-north-korea-has-more-risks-than-benefits-pub-87672

transparency and take measures to reduce the chances of misunderstandings in a crisis. China, Russia, and the U.S.A. have very different nuclear and conventional force structures, which makes it difficult to conclude agreements similar to the Strategic Arms Limitation Talks (SALT)[54] or New Start[55] treaties. This could lead to difficulties on both the scope and the verification mechanisms of future agreements. While parity in strategic nuclear capabilities was used to define the Cold War understanding of strategic stability, the strategic postures of China, Russia and the U.S.A. are increasingly reliant on concepts and capabilities in different operating domains.

The concept of strategic stability has also expanded vertically as there is a greater variety of tools - nuclear and non-nuclear - able to create strategic effects. In addition to the size of nuclear arsenals, today's strategic competition is defined by a race to develop and deploy a range of EDTs, including missile defences, long-range conventional strike weapons, and cyber and counterspace capabilities. Optimists use Cold War logic and argue that the new vulnerabilities created by EDTs will force the great powers to the negotiating table once they recognize that mutual vulnerability is inescapable. However, first-comer advantages are likely to be short-lived and arms-racing incentives reduced as states catch up to one another and develop countermeasures. Furthermore, EDTs provide a significant military advantage to the first to deploy a new technology (quantum computing and "intelligentized" AI, for example). These new capabilities blur the lines between nuclear and conventional warfighting doctrines, and blend nuclear, space, cyber and conventional domains. The complexity of this multidomain strategic environment makes it more difficult to distinguish between stability and instability. The dialogue between the great powers is further complicated by the fact that China, Russia, and the U.S.A. have different interpretations of the military utility of the new domains, and they have developed different concepts for warfighting and escalation control. The future of arms control and strategic stability will be influenced by how these new technologies are exploited by the great powers.

Mr. Rauf ended his comments by noting potential solutions. The priority remains to avoid any use of nuclear weapons thus strategic stability can and must be conceived as a set of provisions that minimize the risk of use of nuclear weapons. Some basic elements for feasible strategic stability engagement include: a degree of mutual restraint, the continued use of the Cold War logic of mutual vulnerability, and a structured mechanism to bring the great powers together, for example an enhanced P5 process.[56] The discussions initiated in the so-called P5 sub-group on nuclear risk reduction should be continued within the framework of the five-year NPT review process.[57] Despite the failure of the NPT preparatory committee session in Vienna in August 2023,[58] it went unnoticed that the five NWS held working level meetings on the sidelines and the chair of the P5 process was passed on to Russia. Finally, the search for arms control agreements in the context for strategic stability and EDT multipliers needs to be pursued as a set of pragmatic measures, such as:

- covering all categories of nuclear weapons/warheads;
- establishing guard rails on AI, cyber and other emerging destabilizing technologies;
- ensuring the survivability of second-strike forces;
- clarifying force postures and limiting the risks of misunderstandings linked to the practice of strategic ambiguity;

[54] See https://www.nti.org/education-center/treaties-and-regimes/strategic-arms-limitation-talks-salt-ii/
[55] See https://www.nti.org/education-center/treaties-and-regimes/treaty-between-the-united-states-of-america-and-the-russian-federation-on-measures-for-the-further-reduction-and-limitation-of-strategic-offensive-arms/
[56] See https://www.europeanleadershipnetwork.org/the-p5-process/
[57] See https://disarmament.unoda.org/wmd/nuclear/npt/
[58] See https://meetings.unoda.org/npt-/treaty-on-the-non-proliferation-of-nuclear-weapons-preparatory-committee-for-the-eleventh-review-conference-first-session-2023

- strengthening all means, cooperative or unilateral, to ensure transparency in armaments and force postures;
- negotiating a follow up to New START through an executive agreement rather than a traditional negotiated treaty that goes at least a third below New START central limits, while retaining New START verification and data exchange protocols; and
- preventing the possibility of surprise attacks.

Discussion

The discussion period opened with a request for reflection on lessons and implications that nuclear weapons and the risks of strategic instability have for the war in Ukraine. It was responded that the Ukraine war shows both that nuclear states are emboldened to take action against weakened states, and the fear of nuclear escalation has created an extraordinary culture of risk aversion, seen, for example, in NATO's decision to not enter the war. This also means that conventional war will likely become nuclear, and that a fundamental change is thus required in both military tactics, and in terms of what the absolute minimum to deter now consists of, as well as in nuclear arms lobbying in these respects. A follow up question was asked about the relationship between Russia and China and its affects on nuclear dialogue. It was responded that Russia and China engage in dialogue based on a number of factors including their economic priorities and relevant support needed from the other. China tends to defer to Russia on nuclear issues. China published a 2003 white paper on its nuclear reduction strategy.[59] Given various common interests, it was asked whether there can be motivation to keep humans involved in AI processes? It was responded that in the civilian area, industry is asking for help for regulation amidst pressure to maintain advantage. Hope lies in the creation of the UN Secretary General's intergovernmental panel because the recognition of vulnerability in this context may only come with catastrophe. A final question was posed concerning whether the N5 process may be a vehicle for improved strategic dialogue between Russia and the U.S.A. It was responded that the N5 has not made proceedings of their consultations transparent, but it has established two working groups on aspects of verification, and on strategic stability. It was noted that during the Cold War, retired military personnel from the U.S.A. and Russia would meet to attempt to navigate tensions, and thus serve as a conduit between the two parties for dialogue despite disagreement. In the contemporary context, there are no such roles where decisions can be assessed in a rational matter. Canada can use its role as a middle power to offer solutions in these areas.

Panel 5 - "What Path Forward for Canada?"

- Moderator: Benjamin Zyla
- Speakers: Senator Marilou McPhedran, Robin Collins

Mr. Robin Collins

In thinking through opportunities for Canada's role in the security challenges of emerging technologies, Mr. Collins observes that some claim that despite AI's enhanced capabilities, they do not render older

[59] See https://www.nti.org/analysis/articles/chinas-white-paper-nonproliferation/

military technologies obsolete.[60] Another perspective holds that AI will drive the development of new technologies and outpace our regulatory systems because of the accelerative nature of AI, the clumsiness of international diplomacy, and the limits of international verification and enforcement regimes.[61] Mr. Collins observes that the world relies on AI in areas of infrastructure and medicine. Yet, artificial intelligence companies outnumber states by the tens of thousands,[62] and AI is at risk for technology breaches. Thus, the need for regulation is urgent.[63] Mr. Collins noted this new reality presents an opportunity to reflect on the prevailing (and expensive and dangerous) assumption that the arms race can go on indefinitely and that a technological edge will be unchallenged from external threats. An alternative approach prioritizes stability requiring allies, competitors, and foes and adversaries alike all maintain only moderate levels of threat protection, for mutual benefit. Dramatically lowering threat levels would result in some level of deterrence but would also reduce provocation, cost, risk, and the diversion of precious resources and human capital, and could still promote non-war solutions to conflicts as they arise. Reflecting on where Canada can contribute to the regulation of technologies of concern, Mr. Collins considered deploying AI itself as a conflict mediator. He asked whether both sides of a conflict would listen to a neutral AI arbitrator that could offer complex but fair solutions to "impenetrable" problems, predict casualties and generational costs, victories or stalemates, and suggest concessions to losing parties. Mr. Collins noted that this would not be painless but mostly casualty-free.

Mr. Collins submitted three queries to ChatBox AI assessing whether AI might be used as a neutral arbitrator directed to affect conflict resolution of a difficult war, and posed three variations of this question: *What is a fair and reasonable resolution to the Russia Ukraine war that takes all sides into consideration and responds to the demand that Crimea remain part of Russia, as well as Russian concerns about Ukraine joining NATO and the European Union?* In all three answers, Crimea and Donbas are returned to Ukraine but the regions give up some jurisdiction to Russia. The solution took approximately 12 seconds. Mr. Collins' query provokes us to ask whether nation state leaders would ever defer to a neutral arbitration of a complex issue even if they agreed that the algorithm parameters could be both comprehensive and "unbiased"? Or will power, tribal loyalties and hatred trump any fair deal? Such a question highlights the hesitancy of our national collectives to collaborate to resolve conflicts before they escalate. Mr. Collins also offered several concrete recommendations on the role Canada can play:[64]

1. Develop strategies on how to implement a code of conduct. One way is through Canada's Artificial Intelligence and Data Act.[65]
2. Devote resources towards combatting disinformation from authoritarian regimes; explore digital rights and protection; enhance trust in the safer deployment of AI technologies. There is an obligation to respond to "digital authoritarianism", electoral interference, and infrastructure disruption.

[60] Stephen Biddle (2023). "Back in the Trenches." Foreign Affairs https://www.foreignaffairs.com/ukraine/back-trenches-technology-warfare
[61] Ian Bremmer and Mustafa Suleyman (2023). "The AI Power Paradox." Foreign Affairs https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox
[62] There are 206 states, but there are 58,000 artificial intelligence companies in the world, with 15,000 of them in the US alone. See https://explodingtopics.com/blog/number-ai-companies
[63] Bremmer and Suleyman (2023) recommend we focus on three urgent institution building options for developing cooperative mechanism: establish a global scientific body to objectively advise governments and international bodies; manage tensions between the two main state players, the USA and China, using verification and monitoring approaches supported by national regulatory and international standard setting bodies; implement censorship to block dangerous AI models.
[64] Here, Mr. Collins draws upon the October 2023 Canadian Governance Internet Forum: The Future We Want. See https://canadianigf.ca/agenda-2/?utm_source=cigi_newsletter&utm_medium=email&utm_campaign=addressing-exposure-to-space-cyber-threats
[65] See https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act

3. Canada holds the 2025 G7 Presidency[66] and can play a role in developing a strategy for multilateral engagement addressing new threats.
4. Promote a Commons-based approach to the coordination of global efforts focused on AI including UNESCO's Ethics of AI project;[67] a 2024 Global Conference on AI and Human Rights;[68] the proposed establishment of a competency framework; an African Union framework;[69] a European Union AI Act.[70] The UK has been building ISO standards, which they call a "pro-innovation approach to AI regulation".[71] Such an approach must address ethical and security obligations through enforceable international treaty-based agreements.
5. Support a high-level advisory body for the UN Secretary-General.
6. Promote AI in support of the UN Sustainable Development Goals.[72]
7. Continue to be an early champion of a Digital Charter (2018) on data[73] and the UN Intergovernmental Panel on Artificial Intelligence,[74] and tie these to the New Agenda for Peace,[75] the Global Digital Compact,[76] and the UN Summit of the Future in 2024.[77]
8. Use its expertise in conflict resolution and confidence building measures in the areas of verification that can be enhanced with new sensory, tracking, reporting, and weapons destruction technologies.

Senator Marilou McPhedran

Senator McPhedran opened her remarks by noting there is little compelling news concerning Canada's role in the use of nuclear weapons and observed that those present in this conference are voices for viable options and potential solutions. Senator McPhedran outlined attempts to push this conversation further as proposed by various stakeholders including Canada's Parliament and Senate, specific MPs, and youth organizations. On the part of Parliament, Senator McPhedran noted that little progress has been made, though it holds the need to pursue nuclear weapons concerns in high regard. A positive sign can be seen in the support of over 30 Senators and 40 Parliamentarians for the International Campaign to Abolish Nuclear Weapons (ICAN) pledge to work towards Canada's signature and ratification of the Treaty on the Prohibition of Nuclear Weapons (TPNW).[78] In addition to Senator McPhedran, two MPs are particularly vocal in support of the need for Canada to commit to banning nuclear weapons: MP Elizabeth May[79] and MP Heather MacPherson.[80] Despite this support, Canada has missed key opportunities to engage in these conversations. One such opportunity was to attend as an Observer at the first Meeting of States Parties to the Treaty held in Vienna, Austria, from 21 to 23 June 2022, but Canada did not attend this meeting. Another was the October 2023 statement made by the Ambassador and Permanent Representative of Canada to the United Nations, Bob Rae, which emphasized the need for leadership and referenced Canada's support of the working group on strengthening the review process, CTBT, and the importance for nuclear countries to engage on these issues, but did not mention

[66] See https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/index.aspx?lang=eng
[67] See https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
[68] See https://www.ai-right-to-life.si/en/2014-conference
[69] See https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging
[70] See https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
[71] See https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
[72] See https://sdgs.un.org/goals
[73] See https://ised-isde.canada.ca/site/innovation-better-canada/sites/default/files/attachments/Digitalcharter_Report_EN.pdf
[74] See https://www.un.org/techenvoy/ai-advisory-body
[75] See https://dppa.un.org/en/a-new-agenda-for-peace
[76] See https://www.un.org/techenvoy/global-digital-compact
[77] See https://www.un.org/en/common-agenda/summit-of-the-future
[78] See https://pledge.icanw.org/full_list_of_pledge_takers
[79] See https://www.ourcommons.ca/PublicationSearch/en/?PubType=37&Item=12031578
[80] See https://twitter.com/HMcPhersonMP/status/1539334969138589696?s=20&t=i0mQXEtv-Tt6lch45WvS-Q

the TPNW. Senator McPhedran noted that Canada's absence in these respects is perplexing, for which she does not have a rational explanation. She stated there exists a strong movement led by young leaders seeking to engage Parliamentarians and build anti-nuclear weapons partnerships. A recent example is the Youth Parliament Nuclear Summit, an initiative led by Reverse the Trend, an organization that aims to mobilise action toward climate security and nuclear disarmament. The Summit brings together youth and stakeholders to discuss "effective strategies promoting nuclear disarmament, climate justice and peace… across all aspects of nuclear policy, including the TPNW, the Nuclear Non-Proliferation Treaty and the Comprehensive Nuclear-Test-Ban Treaty."[81] It is events like these that can amplify this issue to Parliamentarians and encourage cross-party support. This meeting precedes the second Meeting of States Parties to the TPNW convened by UN Secretary-General Guterres for the 27th of November to the 1st of December 2023 at United Nations Headquarters in New York City.[82] Senator McPhedran will attend this meeting and hopes that MPs will also attend. Senator McPhedran ended on a note of apprehension. She stated that advocates are at a stalemate and the only way forward is for Parliament and civil society to work together and push forward difficult questions.

Discussion

The discussion period was opened with a request to consider the establishment of a Canadian Centre on Peace to encourage and harness Canadian intelligence and discussion on these matters. A subsequent comment focused on Rae's choice to not mention the TPNW and it was put forth that there is coalescence amongst NATO countries to stand up in a stronger way against the TPNW now that the NPT is entered into force and gaining momentum. At the NPT meeting in Vienna, Germany, Italy, and the Netherlands made a statement that NATO nuclear weapons have been seamlessly integrated into the NPT. This is not correct and did not happen, and therefore this is an opportunity for Canada and civil society to push back against this narrative. This is an attempt by these states to push against the power of the TPNW and the states and civil society that are backing it. It was responded that the solidarity of NATO is the argument used to justify Canada's absence as an Observer. What is different this time around is that NATO's solidarity has already been breached in this manner. The question now is what side Canada will support, or whether it take a back seat approach. A follow up comment noted that NATO countries are not prepared to join the TPNW in large part because they were not involved in its initial negotiations.

It was then asked whether nuclear abolition was less a realistic goal than non-proliferation, and whether Canada can become a voice in the negotiation of a new treaty on nuclear abolition. It was responded that abolition would require significant resources and would only be feasible if Canada took a leadership role akin to the one it took negotiations on the Responsibility to Protect. Furthermore, Abolition 2000 circulated a proposal[83] that argues the vehicle through which we achieve abolition does not matter; it is abolition that is the goal. There are multiple potential avenues including TPNW, Nuclear Weapons Convention (NWC), or a package of mechanisms. This proposal was distributed to the NPT in 2023 and sent to Global Affairs Canada (GAC) and GAC was receptive but the Government of Canada was not. If Canada is not going to sign the TPNW, then Canada should at least attend the TPNW meeting because this demonstrates Canada's support of the mission of the Treaty despite being unwilling to sign it. This would also demonstrate Canada's support of abolition.

It was asked why there are so few supporting voices in Parliament. It was responded that this issue is indeed on the radar of Conversative members, but that it is essentially is a matter of constituent politics. Thus, civil society partnerships are crucial, and the time is ripe for increased engagement. The

[81] See https://rttreversingthetrend.org/youth-parliament-nuclear-summit
[82] See https://meetings.unoda.org/tpnw/tpnw-msp-2023
[83] See https://www.abolition2000.org/en/news/2023/08/03/nwc-reset-working-paper-presented-to-the-2023-npt-prep-com/

Hill Times[84] will sponsor the upcoming Youth Parliament Nuclear Summit and it is hoped that its engagement with the event will lead to greater awareness across parties in Canadian Parliament. A final question was posed concerning Canada's ability to craft independent foreign policy. It was responded that Canada is weighing whether to attend the TPNW vis-à-vis Canada's perceived solidarity commitments to NATO and the Ukraine war. Canada sometimes is lacking in institutional memory because of staffing churn within Global Affairs Canada, but its opportunity to make a mark now would be to attend the second Meeting of States Parties to the TPNW in November 2023 as an Observer.

Concluding Remarks

Dr. Gheciu and Cesar Jaramillo closed the conference by thanking CIPS and Pugwash for their strong friendship. They ended on a note of optimism and a strong commitment to pursue this discussion. Both remarked that this conversation is far from over and Mr. Jaramillo cautioned participants to remain hopeful as civil society, academia, and political leaders are focused on these issues. Stakeholders are taking active roles in pursing these challenges, which form a political struggle of the highest order.

[84] See https://www.hilltimes.com/

Speaker Biographies

Robin Collins has been active in several civil society organizations since the early 1990s — working mostly on disarmament issues related to nuclear weapons, anti-personnel mines, and cluster munitions. Since 2021 he has been Co-Chair of the Canadian Network to Abolish Nuclear Weapons and Secretary of Canadian Pugwash Group. He is a board member of Rideau Institute and World Federalist Movement—Canada. Collins has published short commentaries about UN reform, peacekeeping, common security, disarmament and a variety of global governance ideas. He has been reviewing books for The Canadian Field-Naturalist journal. He worked in technology companies for 40 years and recently retired, and has a BA in political science from Carleton University.

Dr. Walter Dorn is Professor of Defence Studies at the Royal Military College of Canada (RMC) and the Canadian Forces College (CFC). He teaches officers of rank major to brigadier-general from Canada and about 20 other countries. He specializes in arms control, international criminal law, just war theory, peace operations, treaty verification and enforcement, and the United Nations. As an "operational professor" he participates in field missions and assists international organizations. For instance, he was a UN Electoral Officer for the 1999 referendum in East Timor and a Visiting Professional with the International Criminal Court (ICC) in 2010. He also served as a consultant with the UN's Department of Peacekeeping Operations, including as a member of the Expert Panel on Technology and Innovation in UN Peacekeeping.He is currently doing consulting work for the International Committee of the Red Cross (ICRC) on religions and the rules of armed conflict. He has been active in peace and disarmament NGOs, being the Representative to the UN of Science for Peace since 1983. He served a Chair of Canadian Pugwash for three terms (2008-2013). Two of his books are *Air Power in UN Operations: Wings for Peace* (Ashgate, 2014) and *Keeping Watch: Monitoring, Technology, and Innovation in UN Peace Operations* (UNU Press, 2011). He is also developing digital simulations of peace/peacekeeping operations for training and education (www.peacekeepingsim.net). Website: www.walterdorn.net.

Dr. Alexandra Gheciu is a Professor at the Graduate School of Public and International Affairs. Her publications include, in addition to articles in leading academic journals, several books: *NATO in the ''New Europe': The Politics of International Socialization After the Cold War* (Stanford University Press, 2005); *Securing Civilization? The EU, NATO and the OSCE in the Post-9/11 World* (Oxford University Press, 2008); *The Return of the Public in Global Governance* (co-edited with Jacqueline Best, Cambridge University Press, 2014); *Security Entrepreneurs: Performing Protection in Post-Cold War Europe* (Oxford University Press, 2018); and *The Oxford Handbook of International Security* (co-edited with William Wohlforth, Oxford University Press, 2018). She is a member of the team working on the Global Right project and is writing a new book on NATO in an illiberal world. Prior to joining the University of Ottawa, she was a Research Fellow at the University of Oxford, and a Jean Monnet Fellow at the European University Institute, Florence. She has also been a Senior Research Associate with the Changing Character of War Programme (Oxford University), a Visiting Professor at Sciences Po, Paris and at the Ca' Foscari University of Venice, and the 2022 MINDS Research Fellow at the NATO Defence College (Rome).

Cesar Jaramillo is executive director at Project Ploughshares and Chair of the Canadian Pugwash Group. His focus areas include nuclear disarmament, the protection of civilians in armed conflict, emerging military technologies and conventional weapons controls. As an international civil society representative Cesar has addressed, among others, the UN General Assembly First Committee, the Conference on Disarmament, the UN Committee on the Peaceful Uses of Outer Space, as well as states parties to the Nuclear Non-Proliferation Treaty and to the Arms Trade Treaty. In 2022 Cesar participated in the 10th Review Conference of the Nuclear Non-Proliferation Treaty as a member of the official Canadian government delegation. He has given guest lectures and presentations at academic institutions such as New York University, the National Law University in New Delhi, the China University of Political Science and Law in Beijing, and the University of Toronto. Cesar graduated from the University of Waterloo with an MA in global governance and has bachelor's degrees in honours political science and in journalism. Prior to joining Project Ploughshares, he held a fellowship at the Centre for International Governance Innovation (CIGI).

Dr. Branka Marijan is a senior researcher at Project Ploughshares. Branka leads the research on the military and security implications of emerging technologies. Her work examines ethical concerns regarding the development of autonomous weapons systems and the impact of artificial intelligence and robotics on security provision and trends in warfare. She holds a PhD from the Balsillie School of International Affairs with a specialization in conflict and security. Branka is a lecturer in the Master of Global Affairs program at the Munk School, University of Toronto. Branka is the current chair of the Peace and Conflict Studies Association of Canada. Branka has conducted research on post-conflict societies and published academic articles and reports on the impacts of conflict on civilians and diverse issues of security governance, including security sector reform.

Peggy Mason, President of the Rideau Institute on International Affairs. A former Canadian Ambassador for Disarmament to the UN and an expert on the political/diplomatic aspects of UN peacekeeping training, since June of 2014 Peggy Mason has been the President of the Rideau Institute, an independent, non-profit think tank focusing on research and advocacy in foreign, defence and national security policy. In that capacity, she brings a progressive voice to issues ranging from the imperative of nuclear disarmament to the centrality of UN conflict resolution and the progressive enhancement of international law.

Habib Massoud served for more than 32 years in the Canadian Diplomatic Service. His overseas assignments in Canadian diplomatic posts included Colombia, Croatia, Macedonia, Libya, Lithuania, and Germany. At Global Affairs Canada's headquarters in Ottawa, he served in a number of divisions managing European and international security issues including the Defence Relations Division and the Non-Proliferation and Disarmament Division. Habib was Canada's lead negotiator on the Arms Trade Treaty (ATT) from the start in September 2010 until its conclusion in April 2014. He also led the Canadian delegations to the Missile Technology Control Regime (MTCR), and in talks to achieve a European Union-led International Code of Conduct on the Peaceful Uses of Outer Space. In addition to his diplomatic work for Global Affairs Canada, Habib has also been an international election observer for more than 20 years, participating in election observations missions of the European Union, the Organization for Security and Cooperation in Europe, and in Canadian election observation missions. He has observed Presidential and Parliamentary elections in Kazakhstan, Moldova, Egypt, the Democratic Republic of Congo, the

Palestinian Area, Macedonia, and Croatia. Since retiring from the Canadian Foreign Service, he has published opinion articles in Policy Options and the Globe and Mail.

The Honourable **Marilou McPhedran** is a human rights lawyer, educator, and activist, appointed an independent senator, recommended by Prime Minister Justin Trudeau in November 2016. Marilou was appointed a Member of the Order of Canada in 1985 for her contributions as a young lawyer to Canada's constitution-building through her co-leadership in the 1980s of the Ad Hoc Committee of Canadian Women on the Constitution - the grassroots social and political movement of women across Canada resulting in stronger equality rights in the constitution. In 1985, to enable strategic impact litigation for constitutional intersectional equality rights, she co-founded LEAF, the Women's Legal Education and Action Fund. A pioneer in human rights education, she was the founding Principal of the University of Winnipeg Global College. A founding board member of the Global Network of Women Peacebuilders, she facilitates student access to UN sessions to provide practical skill- building in multilateralism.

Paul Meyer is Fellow in International Security and Adjunct Professor of International Studies at Simon Fraser University in Vancouver (since 2011). Previously, Mr. Meyer had a 35-year career with the Canadian Foreign Service, including serving as Canada's Ambassador to the United Nations and to the Conference on Disarmament in Geneva (2003-2007). He is a Senior Advisor to ICT4Peace, a Fellow of the Outer Space Institute and a Director of the Canadian Pugwash Group. He teaches a course on diplomacy at SFU and writes on issues of nuclear non-proliferation and disarmament, outer space security and international cyber security.

Nisha Shah is an Associate Professor in the School of Political Studies at the University of Ottawa. Her research interests are in the areas of international relations, international security, and political geography, with a particular interest in the history of science and technology in world politics. Her current project, *Calibrating Lethality*, traces the history of the ethics of killing in war through the design and development of weapons. She is currently a co-editor of *The Review of International Studies*.

Tariq Rauf is a Vienna-based expert and consultant on nuclear governance matters, formerly he was the Head of Verification and Security Policy Coordination, Office reporting to the Director General, International Atomic Energy Agency (IAEA); Alternate Head of the IAEA Delegation to NPT Conferences and PrepComs; IAEA Liaison and Point-of-Contact for the Trilateral Initiative, the Plutonium Management and Disposition Agreement, the Fissile Material Control Treaty, the Nuclear Suppliers Group, UNSCR 1540 Committee and (UN) Counter-Terrorism Implementation Task Force; Coordinator of IAEA Multilateral Approaches to the Nuclear Fuel Cycle, and IAEA Forum on Experience of Nuclear-Weapon-Free Zones Relevant for the Middle East. Other prior positions and experience include Member, Group of Eminent Persons for Substantive Advancement of Nuclear Disarmament established by the Foreign Minister of Japan; Consulting Advisor for policy and outreach to the Executive Secretary, Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO); Director, Disarmament and Arms Control, Stockholm International Peace Research Institute; Member of Canada's NPT Delegation; Advisor, Foreign Affairs and National Defence Committees, Parliament of Canada; Director, International Organizations and Nonproliferation Programme, Centre for Nonproliferation Studies, Monterey Institute for International Studies; and Senior Research Associate, Canadian Centre for Arms Control and Disarmament. His education background includes the University of the Panjab (Pakistan); University of London: London School of Economics & Political Science (LSE) and King's College; Carleton University and the University of Toronto in Canada where he was the Ford Foundation Fellow in Dual Expertise: International Security/Arms Control and Soviet-East European Studies.

Srdjan Vucetic is a Professor at the Graduate School of Public and International Affairs and a member of the Centre for International Policy Studies at the University of Ottawa. His research interests are in international security, foreign and defence policy, and the Yugoslav region. Prior to joining the GSPIA, Srdjan was the Randall Dillard Research Fellow in International Studies at Pembroke College, University of Cambridge.

Dr. Jessica West leads research to advance peace and security in outer space through a humanitarian focus on space for all and benefits to people and the planet. As part of this work, she interacts regularly with key United Nations bodies tasked with space security and space safety issues. Related research interests include approaches to peace and disarmament rooted in humanitarian protection and feminist perspectives, as well as the impact of new technologies on space security such as cyber connectivity and artificial intelligence. Jessica holds a Phd in global governance from the Balsillie School of International Affairs where her work focused on linkages between resilience, national security, and public health. She currently holds roles as a Research Fellow at the Kindred Credit Union Centre for Peace Advancement, and as a Senior Fellow at the Centre for International Governance Innovation (CIGI).

Dr. Leah West is an Associate Professor of International Affairs at the Norman Paterson School of International Affairs at Carleton University where she teaches public international law, national security law and counterterrorism. She completed her SJD at the University of Toronto Faculty of Law in 2020 where her research explored the application of criminal, constitutional and international law to state conduct in cyberspace. Leah is the co-author with Craig Forcese of National Security Law (Irwin Law, 2021, 2d Ed) and co-editor with Thomas Juneau and Amarnath Amarasingam of Stress Tested: The COVID-19 Pandemic and Canadian National Security (UCP, 2021). Leah previously served as Counsel with the Department of Justice in the National Security Litigation and Advisory Group where she appeared before the Federal Court in designated proceedings and the Security Intelligence Review Committee. She has also argued before and been cited by the Supreme Court of Canada. Before being called to the Ontario Bar in 2016, Leah clerked for the Honourable Justice Mosley of the Federal Court of Canada. Prior to attending law school, Leah served in the Canadian Armed Forces for ten years as an Armoured Officer; she deployed to Afghanistan in 2010.

Benjamin Zyla is full professor in the School of International Development & Global Studies at the University of Ottawa where he directs the 'Peacebuilding and Local Knowledge network (PLKN) and is the co-director of the Fragile States Research Network (FSRN). A political scientist by training, his work has focused on peacebuilding in fragile and conflict affected societies, post- conflict reconstruction, collective action problems of international (security) organizations, and qualitative methods. He has held teaching and research positions at Harvard University; NATO Defence College; Institute for Advanced Study, Konstanz University; École Normale Supérieure de Lyon; and Stanford University.

Conference Program

The Security Challenges of Emerging Technologies

October 20, 2023 at the University of Ottawa

9:00am - 9:30am: *Introduction and Scene setting Address*

- Welcome: Alexandra Gheciu
- Speaker: Cesar Jaramillo

9:30am - 10:30am: *First Panel – "Cyber Security – the Offense-Defence Dynamic"*

- Moderator: Nisha Shah
- Speakers: Walter Dorn, Leah West

10:30am - 11:00am: *Coffee Break*

11:00am - 12:00pm: *Second Panel – "Artificial Intelligence and Autonomous Weapon Systems"*

- Moderator: Cesar Jaramillo
- Speakers: Branka Marijan, Srdjan Vucetic

12:00pm - 1:30pm: *Lunch break*

1:30pm - 2:30pm: *Third Panel – "The Arms Race in Outer Space – Prevention or Proliferation?"*

- Moderator: Habib Massoud
- Speakers: Jessica West, Paul Meyer

2:30pm - 3:30pm: *Fourth Panel – "Nuclear Weapons and the risks of Strategic Instability"*

- Moderator: Alexandra Gheciu
- Speakers: Tariq Rauf, Peggy Mason

3:30pm - 4:00pm: *Coffee Break*

4:00pm - 5:00pm: *Fifth Panel – "What path forward for Canada?"*

- Moderator: Benjamin Zyla
- Speakers: Senator Marilou McPhedran, Robin Collins

5:00pm - 5:30pm: *Concluding remarks*