“Disruptive Technologies and Nuclear Weapons” Plenary Session 18

63rd Pugwash Conference, November 5, 2025, Hiroshima, Japan

Remarks by Paul Meyer, Canadian Pugwash Group and Simon Fraser University

Perhaps it is fitting to begin this session by noting that nuclear weapons represented a “disruptive technology” when they were unleashed on the world 80 years ago. While the science and engineering behind their creation is no longer cutting edge – they have yet to be eclipsed in their devastating power.

These weapons have at times been subjected to arms control restraints and their numbers reduced, but on other occasions nuclear armed states have abrogated these constraints and have engaged in programs of modernization and/or expansion of their offensive nuclear arsenals. Regrettably our current period is characterized by more of the latter behaviour.

As the core problem of the existence of nuclear weapons and their increased saliency in the policies of those states possessing nuclear weapons and their allies remain with us – we must recognize that this problem can be exacerbated by the application of other technologies to the nuclear weapons complex. The space-nuclear nexus, the cyber-nuclear nexus and the AI-nuclear nexus are three prominent technological realms which could prove dangerously destabilizing for both strategic stability and for maintaining the “taboo” on nuclear weapon use.

As a former diplomat I thought I might best make a contribution to this panel by discussing the prospects for diplomacy to mitigate some of the threats these three technologies pose for international peace and security. While we are daily reminded of the military “hardware” that can be developed through applying these technologies there is far less coverage of the “software” of diplomatic processes designed to promote international cooperation in restricting these technologies from being employed in a destabilizing or escalatory manner. .

A point to bear in mind in considering these three technologies is that they are universal in application and increasingly are employed by a wide range of actors. It is fitting therefore that the United Nations, the most universal of diplomatic forums, has been the focus of much of the inter-governmental discussion to date, although other regional groupings have been active on elements.

Let me take up each of these three technological realms of space, cyber and AI in turn and sketch out for you the current state of play and the prospects for progress in them.

Although the space era can be traced back to 1957 and the launch of Sputnik by the USSR, it was only in 1981, at the initiative of the Soviet Union, that an item on space security was added to the Agenda of the UN General Assembly and its forum for multilateral disarmament negotiations the Conference on Disarmament in Geneva. The item was

entitled “Prevention of an Arms Race in Outer Space” or PAROS for short. Although the 1967 Outer Space Treaty foresaw outer space as a realm for peaceful activity and proscribed the placement of nuclear weapons and other WMD in outer space, state practice from the inception included military activity deemed “non-aggressive”. The crucial role of satellites in providing early warning of any nuclear attack and the fact that any debris created in space would not distinguish between friend or foe induced a certain self-restraint on the part of the small group of space-faring nations. The early development and testing of anti-satellite weapons (ASATs) by the Soviet Union and the United States were essentially shelved for a quarter of a century. We have witnessed more recently a resumption of ASAT testing with China in 2007, the US in 2008, India in 2019 and Russia in 2021 all conducting such debris generating tests. Combined with a deterioration of relations amongst the leading space powers this investment in counter-space capabilities revived concerns that during a crisis an attack against an early warning satellite that was part of a country’s nuclear forces had the potential to trigger a nuclear war.

Diplomats engaged in the UN processes regarding space security, currently focused in an Open-Ended Working Group on PAROS are well aware of these risks not just to the belligerents but to the planet as a whole. As one ambassador noted “no one will escape an armed conflict in space”. Initiatives that have been proposed to date however have taken the form of unilateral declarations supported by one camp and opposed by another. For example, Russia and partners have for several years sponsored a General Assembly resolution on “no first placement of weapons in outer space”. For their part the US and its allies have sponsored a resolution prohibiting the testing of direct ascent ASAT missile testing. These resolutions have served to highlight the lack of common approaches rather than foster them. The OEWG proceedings which are in the first year of its four year mandate have been undermined by increasingly tiresome debates over the merits of legally binding versus non-legally binding measures rather than focusing efforts on devising measures that would bring tangible benefits for sustaining outer space for peaceful activities.

The ideas are on the table – a notable one for strategic stability is agreeing standards for so-called rendezvous and proximity operations in which a satellite contacts or comes close to a satellite belonging to another state. It is proposed that such operations occur only with the prior notification and consent of the other state. Since co-orbital ASATs now figure in the arsenals of states agreement on this measure alone would represent significant progress.

A broader prohibition on interfering with any space-based component of a state’s nuclear forces has also been proposed as a restraint measure of obvious benefit but one which would require wide support amongst nuclear armed states and which would pose verification challenges. In brief I believe the OEWG has the potential for agreeing on substantial measures of cooperative security, but this will require greater political will and a readiness to compromise.

The situation is arguably a little brighter on the cyber security front. Since 1998 the UN General Assembly has been considering the agenda item of Developments in the Field of Information and Telecommunications in the context of international security". Progress has been uneven, but a major accomplishment was the consensus agreement in 2015 on a normative framework for responsible state behaviour in cyberspace. This framework enumerated 11 voluntary norms including the non-targeting by cyber means of critical infrastructure on which the public depends and bans on employing proxies in offensive cyber operations.

The track record of compliance with these measures is not stellar and accountability is elusive when states engage covertly in offensive cyber operations. Still the existence of an agreed normative framework is a helpful reference and the OEWG on cyber security has this July ended its four-year mandate by agreeing a substantive report. A key recommendation is for the establishment of a permanent mechanism at the UN for the ongoing consideration of international cyber security matters. The OEWG was already instrumental in establishing a Point of Contact Directory to facilitate rapid communication amongst states in the event of damaging or suspicious cyber incidents.

It has been realized from the start that offensive cyber operations could pose a major risk to nuclear command and control mechanisms. Penetration and manipulation of computer systems connected with nuclear forces as well as disruption of up and downlinks to space-based assets could be extremely destabilizing. Given that the victim of a penetration cannot know whether the intent is only to exfiltrate data or to damage or destroy functionality any cyber operation directed against nuclear forces is fraught with risk. This has prompted some arms controllers to call for a prohibition against any form of offensive cyber operations directed against such forces. To date however these ideas have not been taken up by the states which could put them into practice.

Looking forward the creation of the "Global Mechanism" in 2026 will provide a much-needed forum for states and stakeholders to raise issues of concern regarding state practice in cyberspace including potential detrimental impacts on strategic stability. The training of a spotlight on the murky world of offensive cyber operation may have some deterrent effects on state conduct, but we are still a long way from codifying specific measures of restraint in this field of operations.

The latest subject to gain a spot on the ever-crowded agenda of the UN is Artificial Intelligence and its military applications. To date much of the UN's discussion has involved conventional autonomous weapon systems and what prohibitions or restrictions may apply to them. Although some states and NGOs such as the "Stop Killer Robots" coalition have sought a ban on fully autonomous weapons this has been resisted by other states interested in exploiting the military usage of AI. In the consensus decision-making context of the UN and in particular the Convention on Certain Conventional Weapons (CCW), under which

auspices the discussions have occurred little progress beyond a general affirmation of the need for meaningful human control of such weapons has happened.

While as noted the deliberations to date have focused on conventional weapon systems everyone is aware of the potential for AI to be employed in the operation of nuclear forces. This topic may become more prominent as stakeholders expand the parameters for discussion. Some states, frustrated by the lack of results stemming from the current CCW discussions, are looking at new mechanisms established via the authority of the UN General Assembly which decides matters on the basis of majority vote rather than consensus.

A positive impulse to UN consideration of the AI governance issue in the military arena arrived with the "Pact for the Future" agreed in September 2024. The pact proposed, in an evident attempt to placate both the opponents and proponents of military AI ,to "continue to assess the existing and potential risks associated with the military applications of artificial intelligence and the possible opportunities throughout their lifecycle". Subsequently the General Assembly tasked the Secretary General with establishing an Independent International Scientific Panel on AI along with initiating an annual Global Dialogue on AI Governance. At the same session, the General Assembly also adopted a resolution (79/239) on "Artificial intelligence in the military domain and its implications for international peace and security" which essentially called for member states to share their views on the topic. The text of the resolution does note "the need for States to implement appropriate safeguards, including measures that relate to human judgment and control over the use of force" which is as relevant to the nuclear domain as it is to the conventional.

It is too early to predict whether any of these mechanisms will generate significant results with respect to military applications in general or regarding nuclear forces in particular. Of course, states can address some of these concerns on a bilateral basis as well as multilaterally. Presidents Biden and Xi at a meeting last November promised to sustain human control over the use of nuclear weapons. According to a White House statement issued at the time: "The two leaders affirmed the need to maintain human control over the decision to use nuclear weapons," The two leaders also stressed the need to consider carefully the potential risks and develop AI technology in the military field in "a prudent and responsible manner."

We can debate the significance of declaratory pronouncements of this kind, especially when one of the leaders making them is no longer in power, but they do serve to put the issue on the international agenda and could prompt complementary action – for example a joint statement of the five NWS along these lines would be welcome. Even if states pledge to maintain human control over nuclear use decisions, can we assume meaningful agency on the part of such commanders when they may be reliant on AI decision support mechanisms?

To conclude, space, cyber and AI all pose risks for strategic stability and diplomats will increasingly be challenged to find ways of mitigating those risks through cooperative security approaches.