ICAN 2017 NOBEL PEACE PRIZE

BRIEFING: Emerging technologies and nuclear weapon risks

Introduction

Technology has transformed armed conflict throughout history. Today, emerging technologies in the fields of offensive cyber capabilities, artificial intelligence and autonomous technologies will have a significant impact on military behaviour.

In the nuclear weapons realm, these technologies add another layer of risk to an already unacceptable level of risk of nuclear weapons use. Mitigation measures that only seek to reduce the additional risk that emerging technologies pose to nuclear weapon use is not an adequate response to the nuclear status quo.

Any use of nuclear weapons, either by intent, accident or miscalculation, will cause catastrophic humanitarian consequences. Only the stigmatisation, prohibition and elimination of nuclear weapons can fully address both new and old nuclear weapons risks and guarantee that nuclear weapons are never used again.

It is critical that policy makers and the public understand the pre-existing dangers of nuclear weapons as well as the added risks posed by emerging technologies that make their elimination all the more urgent.

Cyber Operations, Artificial Intelligence, Autonomous Technology and Nuclear Weapons

Cyber Operations

Countries around the world are investing in new cyber capabilities which threaten to have major implications for nuclear risk.

One of the threats posed by offensive digital technology is the increased uncertainty that it can introduce into the decision to launch a nuclear weapon. There are a few different cyber operations with the potential to impact nuclear weapon decision-making, including:

- data manipulation,
- cyber jamming communications channels or;
- cyber spoofing.[i]

Data manipulation refers to tampering with data in any given system. Cyber jamming refers to disrupting authorized wireless communication. Cyber spoofing describes a device impersonating another to be better positioned to launch attacks. Nuclear command and control refers to the process to order and carry out the launch of a nuclear weapon.

In a 2018 study on cyber security and nuclear weapons, researchers at Chatham House made the assessment that: "The risks of a cyber attack on nuclear weapons systems raise significant doubts about the reliability and integrity of such systems in a time of crisis, regarding the ability to: a) launch a weapon b) prevent an inadvertent attack c) maintain command and control of all military systems d) transmit information and other communications e) maintenance and reliability of such systems."[ii]

Manipulated information in the command and control system could lead decision-makers to launch nuclear weapons. What's more, decision-makers' knowledge that information could be manipulated could make them more ready to use nuclear weapons in a time of crisis.[iii] The fear of an offensive cyber operation preventing the launch of nuclear weapons may result in nuclear-armed states changing their operational protocols to more easily launch nuclear weapons quickly or without the current checks or authorizations.[iv] Such changes compound the risk of unintended launch or detonation as a result of false warnings or a miscalculation.

A number of possible scenarios involving cyber operations could lead to escalation and the launch of a nuclear weapon, based on network and system vulnerabilities and deliberate attempts to compromise nuclear-weapon decision making.

One such scenario which was raised during an ICAN-hosted expert workshop on emerging technologies and nuclear weapons, could be that malware is discovered on a computer system that controls nuclear weapons in a time of crisis and leads to considerable escalation.

Offensive cyber operations could lead to the use of nuclear weapons, even when the cyber attack is not intended to impact nuclear weapons or related infrastructure. Given the entanglement of some conventional and nuclear systems, an intended attack on a conventional system could be interpreted by the victim as an attack on a nuclear system, leading to unintended escalation.[v] An cyber attack on conventional systems, already a dangerous and destabilizing move, could thus have even more drastic consequences.

The threat to the predictability of nuclear-armed actors posed by possible cyber attacks further undermines the credibility of nuclear deterrence. Although the theory of nuclear deterrence has already been discredited for a number of other factors, these new developments are causing even some deterrence proponents to question its ongoing relevance and validity.[vi]

Artificial Intelligence and Autonomous Technologies

While artificial intelligence is not new, the increased application of advanced machine learning and autonomous systems to weapons and defense systems is a recent and concerning trend.[vii] With regard to nuclear weapons, the application of these technologies raise serious questions about the nature of human input and judgement over the world's most dangerous weapons.

Applied machine learning and autonomous systems would result in an increased speed of warfare and therefore an even shorter period in which decision-makers will have to choose whether to launch nuclear weapons or not.[viii] Autonomous systems can also lower the threshold to engage in armed conflict, including nuclear conflict.

There is still a debate about whether to remove human evaluation of data from the decision to launch a nuclear weapon, with several government officials stating that they would never remove human input. However, given recent editorials and debate on the subject, the terrifying possibility of machines being programmed to make this existential decision still exists.[ix]

The process in which advanced machines "choose" a course of action is becoming increasingly opaque as machine learning advances, to the point that these processes are called "black boxes." Therefore, it is difficult for humans to check how and why a machine recommended a course of action to understand if the machine has been compromised, is malfunctioning or its programming resulted in an unlawful or unintentional outcome.[x]

The history of nuclear weapons is riddled with near misses where nuclear war was only averted by a human choosing to disregard false positives presented by machines. One example that demonstrates the importance of having humans in the loop to correct machines, is clear in the story of Stanislav Petrov, who famously ignored the warning presented by nuclear detection technology of incoming U.S. nuclear missiles due to his skepticism of the machine, and in so doing prevented a massive humanitarian catastrophe.[xi]

Will today's nuclear operators be as skeptical of the technology as Petrov was? Or will they be influenced by documented "automation bias" and be overly trusting of new technology?[xii]

Policy makers and the military may also be overly eager to introduce immature technology, such as new advanced machine learning, without fully understanding its implications. In the case of nuclear weapons, this could have deadly consequences.[xiii]

As satellite and other intelligence detection systems become more advanced, it will become more difficult to keep historically concealed nuclear weapons, such as nuclear weapons on submarines, hidden. This could then cause nuclear-armed countries to use all their nuclear weapons earlier in a conflict, given that an adversary would seek to immobilize all known nuclear systems as soon as possible.

Conclusion and Recommendations

Right now, nuclear-armed states are embarking on programmes to rebuild their nuclear arsenals for at least another 60-70 years, despite the ever growing risk of nuclear use. Emerging technologies, like cyber capabilities, autonomous technologies, and artificial intelligence, heighten the existing risks of nuclear weapons use, in both predicted and unpredicted ways. As emerging technologies are increasingly incorporated in military operations, the potential for unintended consequences or mistakes will continue to grow.

There are some steps that could help to counteract the aggravated risks of nuclear use posed by emerging technologies, such as taking steps to increase the decision-making time that leaders have to choose to launch nuclear weapons, including by taking nuclear weapons off of high alert. Laws and norms that regulate autonomous weapons and cyber operations would also be a step in the right direction to reduce some nuclear risks.

But ultimately, none of these risk reduction measures can completely eradicate the new risks posed by emerging technologies to nuclear weapons use, let alone pre-existing threats. For example, there is no way to shield any system completely from a cyber attack. Thus, an adequate policy solution to the new risks of nuclear weapon use posed by cyber weapons cannot be to eliminate the threat of a cyber attack on nuclear systems – that is impossible. It must be to eliminate nuclear weapons themselves.

The unparalleled destructiveness of nuclear weapons means that any use would have catastrophic humanitarian consequences, which are too devastating for any state or international organization to be able to respond to.[xiv] The only way to eliminate the risk posed by nuclear weapons use is to eliminate the nuclear weapons themselves, and the catastrophic humanitarian consequences they present.

Recommendations:

Policy makers must take urgent steps to stigmatise, prohibit and eliminate nuclear weapons by joining the Treaty on the Prohibition of Nuclear Weapons, which offers a clear path forward to a world without nuclear weapons, and encouraging others to do so.

Nuclear-armed states must stop investing in the “modernizing” or rebuilding of their nuclear arsenals, including in the name of making them more “safe” or “secure” from cyber attacks, given the futility of such attempts and the insurmountable risks posed by the mere existence of nuclear weapons.

[i] Beyza Unal and Patricia Lewis, “Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences,” Chatham House, January 2018.
[ii] Beyza Unal and Patricia Lewis.
[iii] Ibid.
[iv] Ibid.
[v] Andrew Futter, “Cyber Threats and Nuclear Weapons,” Royal United Services Institute, July 2016.
[vi] Ward Wilson, “The Myth of Nuclear Deterrence,” The Nonproliferation Review, 2008.
[vii] Paul Scharre, *Army of None: Autonomous Systems and the Nature of Warfare*, April 2018.
[viii] Stockholm International Peace Research Institute, “The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk,” Edited by Vincent Boulanin, May 2019.
[ix] Adam Lowther and Curtis McGiffen, “America Needs a Dead Hand,” War on the Rocks, August 16, 2019.

[x] Stockholm International Peace Research Institute, “The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk.”

[xi] John Borrie, “Cold War Lessons for Automation in in Nuclear Weapons Systems,” SIPRI, May 2019.

[xii] Michael C. Horowitz, “Artificial intelligence and nuclear stability,” SIPRI, May 2019.

[xiii] Edward Geist and Andrew J. Lohn. “How might artificial intelligence affect the risk of nuclear war?” RAND, 2018

[xiv] International Campaign to Abolish Nuclear Weapons, “Unspeakable Suffering – the Humanitarian Impact of Nuclear Weapons,” 2012.