Papers of BAS
Humanities and Social Sciences
Vol. 8, 2021, No. 1

Artificial intelligence and its possible use in international nuclear security law

Anguel Anastassov

Abstract: The paper evaluates the possible implications of artificial intelligence (AI) in some key international nuclear treaties. AI could play a substantive role in the detection of cyberattacks on nuclear systems. However, AI is still an emerging technology that does not allow yet removing the human factor from the decision-making processes in the modern nuclear security realities. States have not reached yet a common understanding about the degree to which current international law would be able to regulate AI developments. A conclusion is made that the prospective first steps in using AI could be to adopt mutually agreed upon arrangements at the level of producers, consumers, and the general public, as well as to develop methodologies to certify AI products. The obvious challenges are related to AI's dependence on a representative, sufficiently large set of data with good quality.

Keywords: artificial intelligence, nuclear stability, nuclear security law, regulatory gap

Introduction

The purpose of the paper is to study the extent to which artificial intelligence (AI) could be used in reducing the nuclear weapon risks in today's world as well as the possible international regulations. The interrelationship among AI, key legal instruments in nuclear security, and measures for its international regulation has not been widely analysed in the specialized literature. Therefore, the novelty of the paper is determined by the subject discussed and in particular the proposed regulatory models of nuclear regulation which could be used to develop control on the AI.

AI is the 60-year-old area of computer science making machines capable to perform tasks normally requiring human intelligence. By nature, it implies the delegation of decision-making from humans to machines. Almost all studies in AI acknowledge that no commonly accepted definition of AI exists, in part because of the diverse approaches to research in the field (Artificial Intelligence and National Security 2019, 1). Machine learning could be understood as a part of AI. The main advantage of machine learning is related to so-called 'deep learning', which can learn on its own while machine learning needs to be operated by the programme. As Irena Ilieva pointed out, "Artificial intelligence is a broad term used for a group of sciences, theories and technologies aimed at improving machines' ability to do things requiring intelligence" (Ilieva 2020, 215).

As in many other areas of modern technologies, AI is already a military reality. Weapons systems guided by AI can make decisions without human intervention and more drastic changes are under development. The prospects of developing fully autonomous weapons driven by AI are already a part of the new global arms race. In 2016, then-US President Obama talked to Wired Magazine and stated that "there could be an algorithm that said, go penetrate the nuclear codes and figure out how to launch some missiles. If that's its only job, if it's self-teaching and it's just an effective algorithm, then you've got problems" (Kircher 2016). The world knows very little about the use of AI in nuclear weapons systems. Russia has brought up the issue publicly by announcing the construction of a fully automated nuclear submarine called Poseidon in March 2018 (Seibt 2019). We can admit that it could be a matter of time before the nuclear powers adopt AI in their weapons systems, if it is not already a reality, in countries such as the USA and China.

Against this background, the legal analysis of the possible impact of AI on the international nuclear security law seems to be an urgent necessity. The question of deployment and disarmament of nuclear weapons systems, as well as the question of AI-augmented offensive and defensive cyber capabilities, is at the centre of the international security debate, and the paper intends to contribute to this debate.

Application of artificial intelligence

The distinction between human and AI may be distorted by developments in human-AI interfaces subject to modern trends of science and technology.

There is an increasing body of evidence that AI[1] will benefit humanity on a wide scale and across many fields. AI could be used to personalize drug treatment, using data accumulated from patient monitoring and existent data, enhancing medical treatment and thereby improving the quality of life and extending life. Self-driving cars would likely see a significant drop in road deaths and injuries - perhaps even saving hundreds of thousands of lives from the

[1] Alan Turing in his 1950 paper, "Computing Machinery and Intelligence", while working at the University of Manchester developed an empirical test of AI. The test involves a human interrogator who is in one room, another human being in a second room, and an artificial entity in a third room. The interrogator is allowed to communicate with the other human and the artificial entity only with a textual device such as a terminal. The interrogator is asked to distinguish the other human from the artificial entity based on answers to questions posed by the interrogator. If the interrogator cannot do this, the Turing test is passed, and we can say that the artificial entity is intelligent (see Neapolitan, Jiang 2018, 2).

nearly 1.3 million deaths and up to 50 million injured that currently occur worldwide each year (McLay 2017, 2).

Any new AI innovation might be used for both military and peaceful purposes since any single algorithm that may provide important economic applications might also lead to the use of nuclear weapons systems - intentionally or unintentionally.

Taking into account the fact that any individual or entity has access to digital data and computing power to use AI, it is difficult to manage the complex nuclear security challenges that emerge. Furthermore, AI algorithms are vulnerable to threat and manipulation, and remote developers develop algorithms on anyone's behalf.

Unlike nuclear energy that is a privilege of the club of a limited number of countries at certain technological levels, the democratization of big data brings universal accessibility. The ethics analysis can differ when we consider offensive or defensive AI military research. In the former, it is ethically unacceptable because the primary purpose is to damage people. The bigger dilemma is defensive AI military research, which serves the public good.

Thus, traditional national and international security concepts related to the violence against respective nations from within or across their geographical boundaries are already outdated and need to be updated. The transition from kinetic delivery to non-kinetic cyber-driven networks facilitates the command, control, communications, computers, intelligence, surveillance, and reconnaissance systems which raises questions about the effectiveness of the current regulatory frameworks.

Artificial intelligence and public international law

AI has no corresponding concept in modern international law. States have not reached yet a common understanding about the degree to which current international law would be able to regulate AI developments. However, AI has already been used in the areas of the use of force, human rights, global health, and intellectual property regimes, among others. Therefore, states could modify the application of existing international law to new realities posed by AI-driven technologies. Technological innovations have driven the developments of public international law throughout history. For instance, among them the following could be mentioned: technologies that enabled the agricultural revolution created a need for exclusive control of land, which led to the tacit expression of concepts of sovereignty and diplomatic relations; advances in ship and navigation technologies during the 16th and 17th centuries stimulated Hugo Grotius to articulate the principle of *mare liberum* (freedom of the seas); the nuclear "shadow" of the Second World War contributed to the establishment of the International Court of Justice and the United Nations (Maas 2019, 6, 7).

A valid question arises as to whether the classic rules of the law of war can be applied to AI and related unmanned combat platforms. In the absence of a specific international legal regime regulating the possible use of AI in nuclear warfare, any State recourse to such operations in peacetime is bound to be subject to currently existing legal norms of self-defense, embodied in the United Nations Charter and international humanitarian law.

The concept of "significant human control" over the automated systems is the centre of the debate. A question arises on the responsibility of the software engineers designing the system when and against whom to target an attack; the operators in the field executing possible attacks; and commanders that knew, or should have known, that subordinates were going to break the law, i.e., commit a crime, but practically did nothing to prevent it. The risk of loss of human control potentially raises the risks for civilians. A question arises as to whether AI systems could make context-specific judgments similar to those of combatants in carrying out attacks under international humanitarian law. Therefore, it is of paramount importance to clarify the level of human control of the unmanned robotic systems taking into account their reliability and predictability.

Given the continuous advancements in autonomous systems matching with AI, any attack is likely to be traced back to its source. However, during its initial stages, it is practically impossible for those in its receiving end to distinguish it successfully from an ordinary hacking attempt, a system failure, or an attack launched by another State's regular troops.

The analysis of what constitutes the use of force through cyber tools matching with AI can be divided according to whether article 2(4) on the prohibition of the use of force should be interpreted by a means-based or an effect-based approach.

Several points could be identified in the analysis of the interphase between AI and international humanitarian law. The classic requirements of necessity and immediacy are practically inherent in any AI attack with a scale large enough to constitute an armed attack. In addition, before the target State takes a step to reply to an AI armed attack with a counterforce, it has to weigh the possibility very carefully because its forcible response might be gravely disproportionate to the attack suffered (Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons 2016).

As specified by the International Court of Justice in the Nicaragua Case, the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States (Case Concerning Military and Paramilitary Activities in and against Nicaragua 1986). Against this background, a cyber-attack using AI could be interpreted as an "armed attack" with all legal and moral consequences.

The international humanitarian law generally regulates the conduct of parties to an armed conflict. The militarization trends of AI have affected international humanitarian law and above all its core principles of distinction, proportionality, and humanity. Taken into consideration the fact that the AI in autonomous weapons systems has not been matured enough, the analysis could be focused on the human decision-making process.

Under the Protocol I of 8 June 1977 Additional to the Geneva Conventions States should conduct legal reviews of new weapons during their development and acquisition, and before their use in armed conflict.

The application of the international humanitarian law to the use of AI does not mean that the AI possible use in nuclear weapons should not be taken into account in the analysis of nuclear strategic stability and possible nuclear arms control negotiations.

Some regulatory models of arms regulation could be used to develop control on the AI such as the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), 1980 Convention on Certain Conventional Weapons (CCW Convention) on lethal autonomous weapon systems (LAWS), and the Tallinn Manual on the International Law Applicable to Cyber Warfare, as examples of how to define and regulate disruptive technologies. The Vienna Document 2011 on Confidence- and Security-Building Measures is another example to be used for updating its coverage.

Within the framework of the CCW Convention, a Group of Governmental Experts was set up with a mandate to explore and agree on possible recommendations and options related to emerging technologies in the area of LAWS. These weapon systems use computer algorithms to independently identify a military target and activate an onboard weapon system to destroy a target without human control of the system. Among the options discussed (a legally binding instrument; no new regulation is needed since the existing international humanitarian law is sufficient to govern the development and use of LAWS; further discussion of the human-machine interphase), a political declaration may be the easiest way to outline important principles such as the necessity of human control in the use of force and importance of human responsibility (Report of the 2018 Session of the Group of Governmental Experts 2018, 7).

The impact of artificial intelligence on nuclear strategic stability

Strategic stability usually refers to a state of affairs in which countries are confident that their adversaries would not be able to undermine their nuclear deterrent capability (Podvig 2012).

Some authors arguably make some parallels between the modern development of AI and the development of nuclear weapons systems by the Cold War superpowers. These authors describe nuclear weapons as a way of compensating for the relative disadvantages of US conventional weaponry against the USSR. Currently, the AI is indicated as a ‘third offset’ strategy, following the 1970s development of information technologies as a ‘second offset’ strategy (Kenneth 2018, 7-32).

As the world enters the post-cold era, the strategic stability was equated with the relationships between the two nuclear superpowers, Russia and the USA, which has been gradually augmented by regional nuclear rivalries and confrontations. Moreover, strategic stability becomes a concept with multiple drivers such as nuclear terrorism, development of modern conventional weapons, cybersecurity, regional conflicts, energy issues, as well as the level of scientific, technological, and economic development (Cuihong 2019, 63-64).

The fundamental role of AI occurs via core competencies such as cognition, prediction, decision-making, and provision of an integrated solution for complex activities. Applications that can empower nuclear weapons systems include environmental detection, target location, early warning, air and space missile defense systems, nuclear weapon command systems, and protective systems for nuclear storage and transportation equipment.

A question arises as to whether the possible handing over control of nuclear weapons to AI could be seen by some as a necessary update of deterrence concept to modern-day technology. Nuclear and AI experts seem to agree that AI may destabilize the nuclear strategic stability and increase the risk of nuclear attack (Geist, Lohn 2018). Hence, AI has been recognized as another field of common interest of the modern world in addition to the proliferation of nuclear weapons and climate change among others.

The AI could be applied to detect cyberattacks and maintain recovery capabilities, which would improve the strategic stability through effective cyber deterrence. The first steps in the formation of a cyberspace control system on a bilateral basis has been marked by the agreements between China and Russia on safeguarding international information security, which includes a pledge not to engage in cyberattacks against each other, and between China and the USA not to attack each other's critical infrastructure (Xiang 2019, 18).

The recent advancement in military AI has a marked impact on nuclear strategic stability on both offensive and defensive sides. Closely linked to AI in the strategic areas are cyber operations. AI can be used to detect and possibly respond to cyberattacks that cannot be detected by human beings. Arguably, a weaker State can use AI to reinforce its conventional and nuclear military potential and apply asymmetric approaches to provoke conflicts.

Artificial intelligence and nuclear military systems

Currently, there are not many cases of using AI in nuclear weapons systems referred to in the open literature. One example is Poseidon, which is designed to hit coastal cities with a 2-megaton warhead, around 133 times more powerful than the bomb dropped on Hiroshima. It is often described as an autonomous underwater vehicle, and as an Intercontinental Nuclear-Powered Nuclear-Armed Autonomous Torpedo (Sutton 2019). AI could play a substantive role in the detection of cyberattacks on nuclear weapons systems. The obvious challenges are related to the dependence of AI on a representative, sufficiently large set of training data with good quality. If this is not the case, the system might misinform human decisions and actions. Moreover, studies are demonstrating that it is easy to produce images that are completely unrecognizable to humans, but that state-of-the-art deep neural networks believe to be recognizable objects with 99.99% confidence (Nguyen, Yosinski, Clune 2015). This point makes machine learning systems easily fooled and their use in military circumstances highly inappropriate.

The existence of new technologies, such as cyber capabilities matching with AI against command-and-control centres in particular can endanger nuclear security as well, leading to unintended escalation. Cyber and AI are developing so fast that the question arises as to whether the usual action-reaction cycle applies.

We share the views of those that are not optimistic to rely strongly on the integration of AI with nuclear command, control, and communications. Both the USA and Russia have experienced systems such as the Soviet Perimeter and the American Survivable Adaptive Planning Experiment (SAPE) in the 1980s. The Perimeter relied on a network of sensors to detect nuclear explosions and delegated launch weapons authority to lower-level officers if the communication line to the General Staff went dead. SAPE did not have direct launch authority either but would translate data into nuclear targeting plans to be transmitted to manned B-2 bombers featuring low observable stealth technology designed for penetrating dense anti-aircraft defenses.

An increasing body of evidence about the dangers to automate the launch of nuclear weapons in the past, as well as the current problems with self-driving car technology, for instance, has confirmed that AI is a nascent technology that does not allow yet to remove the human factor from the decision-making process (Farabaugh 2019).

Artificial intelligence and nuclear non-proliferation regime

AI can detect signs of nuclear weapons testing banned under the *Comprehensive Nuclear-Test-Ban Treaty* (CTBT). The Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) has taken the initiative to implement software that uses state of the art machine learning and AI to complement the established analysis tools (Nakamitsu 2019). The use of machine learning and AI increases the quality of the data and analysis provided to States. This, in turn, strengthens confidence in the CTBT-related International Monitoring System and the nuclear non-proliferation regime more generally. The principal obstacles to a rapid instantiation of machine learning methods within an operational context, however, are the availability of raw data for testing during algorithm development and the difficulty of evaluating and benchmarking the impact of local improvements on the overall system. A programmatic construct has already been suggested for overcoming these hurdles by proposing to coordinate and drive data-related research and development initiatives under the auspices of the CTBTO, for the evolution and evaluation of next-generation data processing methods for CTBT verification (Russell, Vaidya, Le Bras 2010).

The International Atomic Energy Agency, as a global player for nuclear cooperation, is using the enormous potential of AI to help accelerate the secure and peaceful uses of nuclear technologies towards the United Nations' Sustainable Development Goals. The nuclear industry, which has to deal with a huge amount of data may benefit from AI in terms of efficient analysis of complex situations, reducing the rate of errors, drawing adequate findings and conclusions by right data crossing, and improving the decision-making process. However, the AI would not be able to replace nuclear non-proliferation inspectors or analysts at this stage.

Is it possible to fill in the regulatory gap?

It should be noted that the Internet has been developed free of any intergovernmental regulation. AI is a typical dual-use area and its regulation, along with awareness and knowledge, is not an easy task. Taking into consideration the specifics of the AI, it makes sense to suggest that States should be proactive in regulation instead of reactive.

AI arms control might be impossible to be regulated most effectively. Henri Kissinger, former US Secretary of State is of the view that it may be a lot harder to control the development of AI weapons than nuclear ones. He wrote, "Philosophically, intellectually - in every way - human society is unprepared for the rise of artificial intelligence" (Knight 2021). The struggle to end nuclear testing, for instance, is six decades old. Initial efforts to prevent the spread of nuclear weapons and weapons technology dated back to 1946. In 1970, the *Treaty on the Non-Proliferation of Nuclear Weapons* (NPT) entered into force and the NPT Parties met in May 1995 and agreed to extend the treaty indefinitely.

It is worth pointing out a thought, which should not raise particular questions or doubts. In principle, any norm needs to be applied in the newly emerging circumstances, which raises questions of its interpretation and possible update in the first place. Certainly, setting up completely new legal norms and their implementation by respective member States and/or intergovernmental organization is an option, which however presupposes the agreement of all interested actors, which is not an easy task.

Even though it is impossible to reverse the advances of AI development and their possible applications in nuclear weapons systems, it is still not too late to work out the rules of an arms race involving this technology. One example, which could be studied, is the experience of Soviet-American agreements when anti-ballistic missile (ABM) technologies were introduced in the 1970s. The Soviet Union and the United States agreed to abandon plans to field more advanced anti-ballistic missile technologies as evidenced by the ABM treaty, which remained in force until 2002.

The development of nuclear-powered unmanned underwater vehicles has the potential for fallout of long-lived isotopes into the biosphere. It violates Art. VI of the NPT, which obliges each of the parties to pursue negotiations in nuclear disarmament. Besides, the operation of unmanned systems would involve equipment breakdowns resulting in significant radioactive contamination of seawater. This raises challenges to the application of the 1986 *Convention on Early Notification of a Nuclear Accident*. The Convention establishes a notification system for nuclear accidents from which a release of radioactive material occurs or is likely to occur and which has resulted in an international transboundary release that could be of radiological safety significance for another State. Therefore, the update of this legal instrument seems logical and timely.

The numerous peaceful applications of AI could serve as a test for reliability before using them in strategies for launching a nuclear arms attack, which is still a part of the worst-case scenarios today.

Some initiatives to control AI have been taken at various multinational fora. Leading the debate at the EU level, the European Parliament, for instance, adopted its own-initiative-report on a Comprehensive European industrial policy on artificial intelligence and robotics in February 2019. The European Commission adopted on 25 May 2018 a Communication on Artificial Intelligence for Europe laying down the European approach to make the most out of the opportunities offered by the AI and address the challenges AI brings (Ilieva 2020, 216). The OECD Principles on Artificial Intelligence were adopted in May 2019. They promote AI that is innovative and trustworthy and respects human rights and democratic values. In a report published in 2018, the Organization of American States highlighted the importance of Emerging Digital Technologies, such as Big Data, Machine Learning, or Artificial Intelligence for the prevention of cyberattacks.

The United Nations Interregional Crime and Justice Research Institute (UNICRI) established a centre on AI and robotics in early 2015. UNICRI has developed a large international network of stakeholders with whom it collaborates (Butcher, Beridze 2019, 88-96).

Various regulatory approaches have been explored by institutions such as the Group of Governmental Experts (GGE) within the framework of the United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects; United Nations Institute for Disarmament Research, Stockholm International Peace Research Institute, the International Committee of the Red Cross, the International Committee for Robot Arms Control, among many others. There are numerous authoritative studies, including the *Tallinn Manual on the International Law Applicable to Cyber Operations* (Schmitt 2017), which offer good examples of an academic legal approach for addressing military AI.

The prospective first steps in using AI could be to adopt mutually agreed upon arrangements at the level of producers, consumers, and the general public, as well as to develop methodologies to certify AI products. The European Commission has already taken the lead in ensuring an appropriate ethical and legal AI framework including setting AI ethics guidelines; issuance of guidance on the Product Liability Directive, as well as a separate report on the broader implications for, potential gaps in and orientations for, the liability and safety frameworks for AI; support research in the development of explainable AI and implement a pilot project proposed by the European Parliament on Algorithmic Awareness Building (EC Commission 2018).

Just as international trade standards have been established with the World Trade Organization, there are ideas to set up a Cyber and Artificial Intelligence Organization (CAIO) that could focus on establishing international regulations, standards, and fair rules for the evolving digital economy (Fricke 2020, 6).

Conclusion

The use of AI in nuclear security systems could make the world safer and unpredictable. Therefore, the debate on possible regulation of AI should continue. One of the options to be explored as a starting point could be to negotiate an additional protocol to an existing international agreement, for instance, the New START (Strategic Arms Reduction Treaty) between the USA and Russian Federation which was renewed in 2021.

As with the early days of nuclear weapons, regulations will likely follow technology, with legally binding norms materializing still later. This is because the advantages of possessing weaponized AI might be available, but there could be obvious problems in distinguishing legitimate and illegitimate targets in the international nuclear security law.

References

Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons 2016: Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 1996, I. C. J. Rep. 226, 245 para 41. Also, The Iranian Oil Platforms Case, 2003, I. C. J. Rep. 226, 245 para 41.

Artificial Intelligence and National Security 2019: Artificial Intelligence and National Security. Congressional Research Service. CRS Report prepared for Members and Committees of Congress. Updated 21 November 2019, p. 1.

Butcher, Beridze 2019: J. Butcher, I. Beridze. What is the state of artificial intelligence governance globally? - The RUSI Journal, 164, 29 November 2019, 88-96. Available from: https://www.tandfonline.com/doi/full/10.1080/03071847.2019.1694260?scroll=top&needAccess=true [Accessed: 15 February 2021].

Case Concerning Military and Paramilitary Activities in and against Nicaragua 1986: Case Concerning Military and Paramilitary Activities in and against Nicaragua (Merits), 1986 I. C. J. Reports 14, 103 para 195.

Cuihong 2019: C. Cuihong. The shaping of strategic stability by artificial intelligence. - In: L. Saalman (ed.). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. 2. East Asian Perspectives. Stockholm International Peace Research Institute, 2019, 54-77.

EC Commission 2018: Artificial Intelligence for Europe, EC Commission COM, 2018, 25 April 2018. Available from: https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe [Accessed: 15 February 2021].

Farabaugh 2019: B. Farabaugh. Bad idea: Integrating artificial intelligence with nuclear command, control, and communications. - In: Defense360°. Center for Strategic and International Studies, 3 December 2019, last modified 3 December, 2019. Available from: https://defense360.csis.org/bad-idea-integrating-artificial-intelligence-with-nuclear-command-control-and-communications/ [Accessed: 15 February 2021].

Fricke 2020: B. Fricke. Artificial Intelligence, 5G and the Future Balance of Power. (Facts and Findings, January 2020, 378). Berlin: Konrad Adenauer Stiftung, 2020.

Geist, Lohn 2018: E. Geist, A. J. Lohn. How might artificial intelligence affect the risk of nuclear war? Santa Monica: RAND Corporation, 2018. Available from: https://www.rand.org/pubs/perspectives/PE296.html [Accessed: 15 February 2021].

Ilieva 2020: И. Илиева. Върховенството на правото и изкуственият интелект. - Известия. Списание на Икономически университет - Варна, 64, 2020, 3, 210-226. (I. Ilieva. Varhovenstvoto na pravoto i izkustveniyat intelekt. - Izvestiya. Spisanie na Ikonomicheski universitet - Varna, 64, 2020, 3, 210-226.)

Kenneth 2018: P. Kenneth. Artificial intelligence: A revolution in strategic affairs? - Survival, October-November, 2018, 7-32.

Kircher 2016: M. M. Kircher. Obama on the risks of AI: 'You just gotta have somebody close to the power cord'. - Intelligencer, 12 October 2016. Available from: https://nymag.com/intelligencer/2016/10/barack-obama-talks-artificial-intelligence-in-wired.html [Accessed: 15 February 2021].

Knight 2021: W. Knight. AI arms control may not be possible, warns Henry Kissinger. - MIT Technology Review, 2021. Available from: https://www.technologyreview.com/f/613059/ai-arms-control-may-not-be-possible-warns-henry-kissinger/ [Accessed: 15 February 2021].

Maas 2019: M. Maas. International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order. - Melbourne Journal of International Law, 20, August 2019, 1, 1-29.

McLay 2017: R. McLay. Managing the Rise of Artificial Intelligence. Available from: https://tech.humanrights.gov.au/sites/default/files/inline-files/100%20-%20Ron%20McLay.pdf [Accessed: 15 February 2021].

Nakamitsu 2019: I. Nakamitsu. UN High Representative for Disarmament Affairs (UNODA) addressing the High-Level Panel "CTBT: Science and Technology in a Changing World" on 24 June at Hofburg Palace, Vienna, as part of the Science and Technology Conference 2019 (SnT2019) 24 June - 28 June 2019.

Neapolitan, Jiang 2018: R. E. Neapolitan, X. Jiang. Artificial Intelligence. With an Introduction to Machine Learning. 2nd ed. Chapman and Hall/CRC, 2018.

Nguyen, Yosinski, Clune 2015: A. Nguyen, J. Yosinski, J. Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. - In: Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015. Available from: https://www.researchgate.net/publication/307560165_Deep_neural_networks_are_easily_fooled_High_confidence_predictions_for_unrecognizable_images [Accessed: 15 February 2021].

Podvig 2012: P. Podvig, The myth of strategic stability. - Bulleting of Atomic Scientists, 31 October 2012.

Report of the 2018 Session of the Group of Governmental Experts 2018: Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems. Doc. CCW/GGE.1/2018/3, 23 October 2018.

Russell, Vaidya, Le Bras: 2010: S. Russell, S. Vaidya, R. Le Bras. Machine learning for Comprehensive Nuclear-Test-Ban Treaty monitoring. CTBTO Spectrum, 14, April, 2010.

Schmitt 2017: M. N. Schmitt (ed). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defense Centre of Excellence. Cambridge: Cambridge University Press, 2017. 641 pp.

Seibt 2019: S. Seibt. From the A-bomb to the AI bomb, nuclear weapons' problematic evolution. - In: France 24, 5 October 2019. Available from: https://www.france24.com/en/20190510-nuclear-weapons-artificial-intelligence-ai-missiles-bombs-technology-military [Accessed: 15 February 2021].

Sutton 2019: H. I. Sutton. Video suggests Russia's Poseidon nuclear-powered drone has a seabed-launched version. - Forbes, 17 November 2019. Available from: https://www.forbes.com/sites/hisutton/2019/11/17/video-suggests-russias-poseidon-nuclear-powered-drone-has-a-seabed-launched-version/#2f5c41585b6c [Accessed: 15 February 2021].

Xiang 2019: L. Xiang. Artificial intelligence and its impact on weaponization and arms control. - In: L. Saalman (ed.). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. 2. East Asian Perspectives. Stockholm International Peace Research Institute, 2019, 13-19.

Assoc. Prof. Anguel Anastassov, Dr. Jur. Sc., PhD
Institute for the State and the Law
Bulgarian Academy of Sciences
4 Serdika Str.
1000 Sofia, Bulgaria
Email: anguelanastassov@gmail.com