The Perils of AI for Nuclear Deterrence

Syed Sadam Hussain Shah[*]

Abstract

The use of artificial intelligence (AI) in nuclear affairs could be potentially dangerous. Quantum computing and AI based detection systems, speedy delivery platforms, revolution in remote sensing and precision targeting will challenge hardening, concealment, and survivability of the command and control, delivery platforms, weapons, decision makers and strategic assets.[1] Therefore, the future nuclear forces and arsenals are likely to be more ready to use, decision making time urgent and nuclear doctrines are likely to be conceptually aggressive. However, AI inferior states may increase the number of their nuclear warheads to ensure a retaliatory strike, thus raising proliferation concerns. Moreover, these states will also be compelled to use cyber offences and time urgent postures as countermeasures. On the other hand, AI superior states may resort to counterforce first strike to ensure superiority in a nuclear war. This study will particularly explore how AI would increase the risk of a nuclear war, and impact the nuclear deterrence concepts.

Keywords

Artificial intelligence, perils, hacking, autonomous weapons, nuclear command and control, nuclear deterrence.

Introduction

Advancements in AI have raised both hopes and fears. The use of AI in nuclear matters is making the survival of nuclear forces, and command, and control of nuclear weapons more challenging. This has serious implications for nuclear deterrence and strategic stability. The

[*] Syed Sadam Hussain Shah is a Research Assistant at the Center for International Strategic Studies (CISS), Islamabad.

fast [quantum] AI based detection systems will provide more reliable, and accurate information about adversary's nuclear forces, decision makers, command and control systems and strategic assets. Furthermore, autonomous launch platforms and speedy weapons will ensure timely targeting. Therefore, these technologies will give a sense of confidence to nuclear states to move towards time urgent and 'ready to use' postures. This could be destabilizing, as it would be difficult to identify and destroy all of the enemy weapons in a first strike. Some weapons are likely to survive, and a retaliatory strike is likely to result in mutually assured destruction (MAD). Moreover, a state possessing less AI capability may resort to using its nuclear arsenal first to avoid their detection and the possibility of decapitation.[2]

Quantum computers, which are more efficient and faster than supercomputers will further enhance AI-based intelligent processing, big data analysis, image recognition, and remote sensing capabilities. At the same time, these systems are vulnerable to cyber-attacks, which can bring about catastrophic outcomes. Imagine what will happen if a hacker operates an autonomous nuclear delivery platform? What if a hacker launches a nuclear attack in peacetime? What if autonomous platforms launch an attack on the wrong country due to malfunction? What if the data set is not properly trained? What if the data set is tampered with? In such situations, AI can misguide humans in decision-making and start an unintended nuclear war.

There can be a situation when due to malfunction or a deliberate hack; the machine orders the wrong launch of nuclear weapons. If this happens, the attributability of attack may pose a big legal and ethical problem. To avoid such a situation from emerging, there is a need to balance the AI developments with laws, safety, and reliability standards. Human control over the weapons of mass destruction should be an essential and necessary part of the regime to control AI use.

The possibility of terrorists getting their hands on the cheaper drones that can travel hundreds of miles and deliver the payloads pose a potent threat to the security of the state's command and control systems and its sensitive installations. A swarm of thousand drones can be difficult to deal with; even any advanced air force would face difficulties. What if terrorists operate these drones carrying smart bombs? This will particularly be a challenge for security organizations to deal with.

This essay will primarily discuss the risks associated with the use of AI in nuclear weapons, besides how the autonomous weapons, AI based delivery platforms, and other systems will impact the concept of nuclear deterrence.

Defining artificial intelligence (AI)

There are many definitions of AI given by researchers. However, it is essential first to differentiate between three overlapping concepts Machine Learning (ML), Deep Learning (DL), and Artificial Intelligence (AI). Although these concepts overlap in some domains, they are not the same. DL is a subset of ML, and ML is a subset of AI.[3] ML can simply be defined as the algorithms that empower computers to learn by themselves based on the available data. DL is the next level of development of ML. It works like a human brain. Deep learning algorithms can be taught to do the same tasks for computers, which the human brain does for humans.[4] However, the goal of AI is to make computers and machines learn from experience, think like a human brain and reason on their own. For this purpose, artificial neural networks use math and algorithms (computer programs) to impersonate the processes of the human brain to reason independently.[5] There is not a single agreed definition of AI among researchers, but few definitions offer a better explanation. For instance, the US companion bill defined AI as "Any artificial system that performs tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their experience and improve their performance…"[6] William A. Carter from

CSIS defines Machine Intelligence (MI) as “MI refers to machines’ ability to perform tasks that would normally require human intelligence. Computer scientists and mathematicians develop MI systems by imparting the ability to find patterns in large data sets to computers (machine learning).”[7] Stanford’s Researcher, John McCarthy defines AI, as “Artificial Intelligence is the science and engineering of making intelligent machines, especially intelligent computer programs. Artificial Intelligence is related to the task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.”[8]

Hacking AI

AI will be increasingly used in a wide spectrum of organized human activities in future including nuclear, military, commercial and social organizations.[9] However, the possibility that AI can be hacked is all-real. Adversarial machine learning (AMI) can hack AI by tampering datasets or the physical environment. The following are a few of the methods used in hacking machine learning and artificial intelligence.

i. **Tricking a neural network:** The technique is used to trick a neural network or to fool it into seeing something that is not there (misclassification).[10]

ii. **Evasion attack:** In an evasion attack, the hacker adjusts testing samples during the early testing phase, but does not involve any influence over the training data.[11] It is like an input that looks the same as the original to an individual.[12]

iii. **Poisoning attack:** In this attack, the hacker poisons the original data by injecting his own samples to hijack the whole learning process. [13]

iv. **Exploratory attacks:** Hackers try to access the knowledge about the learning algorithm of the system and patterns in the training data sets, which is then used to launch an attack in later phases.[14]

v. **Data modification:** In this case, a hacker does not have access to the learning data, but has full access to the training data. The hacker poisons the training data before it is used for the training model.[15]

vi. **Logic corruption:** It is a technique used by a hacker or malicious actor to alter the learning logic and hijacking or controlling the whole model.[16]

The perils of AI for nuclear deterrence

AI based platforms and other emerging technologies are likely to adversely affect nuclear deterrence. States will have difficulties to deal with robots capable of autonomously launching an attack. The scenarios discussed above are futuristic but possible. AI based detection systems will be able to identify enemy's land, air, and sea based nuclear forces, and faster precision guided delivery vehicles will ensure their timely destruction. This means that these systems will not only impair the second strike capability of a state but will also make its ability to credibly communicate the threat questionable. This may result in deterrence breakdown. The following are some of the key AI based challenges to nuclear deterrence.

Conventional threats

The use of AI based conventional technologies will perhaps be more destabilizing for nuclear deterrence. Quantum-AI based remote sensing, intelligent locating, accurate targeting, speedy image processing, efficiency and speed of AI powered weapons will increase their efficacy as technology improves. This will increase the reaction time and will make survivability of nuclear forces, hardening and concealment even more difficult.

In addition, autonomous terrain scanning platforms based on faster image processing algorithms will be useable in identifying enemy nuclear and ground forces in crisis or peacetime. US Air force will soon have AI powered pilots, who can better manage the flood of information, make informed decisions during the course of their missions, and do a better job in image processing to identify targets on the ground.[17]

AI based conventional weapons will have an advantage over human conventional operations. During the simulation exercise at the US air force research laboratory (AFRL), AI platform alpha (a software used to operate autonomous flying jets) defeated all other opponents including expert US pilots by using fuzzy tree methodology.[18] This happened even when in several circumstances alpha was disadvantaged with respect to air technology, payloads, and aircraft model.[19]

The faster and more accurate delivery platforms like hypersonic missiles, combined with advanced AI algorithms will generate a greater sense of confidence in a state's ability to strike first. For instance, hypersonic cruise missiles coupled with the AI guidance system will take only a few minutes to reach their targets. This will not only add complexity to the decision-making, but states with lesser or no AI based capabilities may resort to the first strike in order to avoid the threat of decapitation or to offset the disadvantage of technological asymmetry. In any case, the use of conventional AI would question the state of mind and perceptions on both sides, and would further deteriorate the nuclear deterrence and strategic stability.

AI decision making and nuclear deterrence

Availability of enough time to verify the attack and decide responses are critical in nuclear decision making. However, decision makers in the chain of command at various levels are under information overload, time urgency, moral considerations, and many other stresses.[20] Fast and difficult to detect weapons like hypersonic cruise missiles have constrained time distances, and the reaction time for the decision makers. AI provides many advantages over humans in overcoming these stresses. Processing and making sense of big data, and informed decisions making would be done using AI. In addition, fast hardware processors and software based on quantum computing will accelerate the completion of tasks for AI based platforms including decision making in the future.

Nevertheless, relying on autonomous and faster decision making systems, in a response mode, could be disastrous for several key reasons. The adversary state may use its arsenal first in order to avoid the possibility of a decapitation strike as noted earlier. Moreover, AI decision-making system may resort to any of the possible conclusions set by an attacker. Likewise, decision-making can be affected by false and possibly tempered information. In addition, huge data sets for algorithms in case of nuclear launches would be needed (data training problem particularly occurs in case of deep learning algorithms) and simply the automation data biases may invoke irreversible decisions.

Autonomous platforms and nuclear deterrence

Autonomous delivery platforms could be unmanned sea, air, and land based including aircraft, submarines, and ground vehicles carrying nuclear weapons. [21] Although some scholars believe that autonomous delivery platforms will ensure the credibility of nuclear deterrence by ensuring a timely retaliation,[22] this could be destabilizing at the same time. An adversary may perceive, the patrolling of an autonomous vehicle carrying nuclear weapons, as a nuclear attack and may strike first in order to avoid the threat of decapitation in fear or haste. Autonomous vehicles would be pre-programmed, and weapons would already be mated with delivery platforms, which will be a huge challenge for any nuclear state in ensuring positive and negative control of such weapons. There could be a case when an unmanned missile delivery vehicle launches the nuclear attack accidentally, unnecessarily, or based on any pre-condition set by malicious actors. Similarly, an autonomous nuclear AI machine may be compromised.

AI detection systems and nuclear deterrence

Quantum computing will double the efficiency of AI based Intelligence, Surveillance, Reconnaissance (ISR) capabilities. These technologies will be absolute in processing, and analyzing information and actionable intelligence for military/nuclear decision makers.[23] AI based computers can detect patterns in thousands of photos that a human eye may never be able to see and make sense of. [24]

Although AI-powered ISR at land, sea, or in space will help in obtaining accurate information about an enemy (enemy targets, C3, military, and nuclear facilities), and maintaining a decisive military and strategic superiority, it will doubt the survivability and enemy state's ability to strike back.

The AI-powered ISR capability may deceive a state by giving it a false sense of confidence in using its nuclear arsenal first to decapitate the enemy state. Many of the enemy's weapons may still survive, thus resulting in a nuclear exchange. Against such eventuality, the state with less ISR may have no other option but to increase the number of its missiles and nuclear weapons. These developments will not only destabilize the strategic stability but also increase the prospects of a nuclear arms race. However, if both states acquire the ability to have real-time intelligence regarding the adversary's nuclear capabilities and operational strategy, it will lead to a stable situation.

A mix of manned and unmanned submarines, undersea vehicles, and a network of sensors would provide timely and accurate information about the enemy's activities underwater.[25] The sea leg of any nuclear deterrent, however, is considered as the credible second-strike capability of a state. Detection of sea-based arsenal will weaken the nuclear deterrent of any state, which could have destabilizing international security implications.

AI cyber threats and nuclear deterrence

Spoofing is useful to fool a target by pretending to be the original source. In nuclear matters, it can be used to access top-secret information or for ordering a false nuclear launch or to expose the system's vulnerabilities. [26] However, with the inception of AI and the use of speech synthesis, and faking voice commands, spoofing has been revolutionized in recent years. An AI hacker can lure in more targets quantitatively, and qualitatively than humans. Zero Fox, an IT security company conducted research to compare the efficiency of artificial and natural intelligence by sending different users a hacking malicious link. Artificial hacker (Ah) was taught to design and implement its own phishing bait, unlike Mr. Thomas Fox-Brewster who participated in the experiment. Ah succeeded in luring 275 victims at the rate of 6.75 tweets per minute, and Thomas could only target 49 users and pump out 1.075 tweets per minute.[27] [28]

Malicious use of AI in spoofing makes nuclear decision-making and communication systems quite vulnerable. If several fake early-warnings appear to be real, will the commander-in-charge of the nuclear weapons order the launch? Similarly, individuals working on sensitive information may mistakenly provide secret information to an AI hacker. The threats of cyber-spoofing are not recent. Emanating from threats, the scale and scope of attacks and methods are not only diverse but also real.

It happened in 1983 when the algorithm of Early Warning System (EWs) wrongly sensed incoming missiles, a warning sounded multiple times; however, the officer-in-charge Stanislav Petrov prevented the imminent crisis by trusting his instincts and not the alarm bell. [29]

The rise in the use of autonomous weapons and systems will also drive inferior AI adversaries' interest in using cyber countermeasures. [30] Every software run machine is vulnerable to attack, and particularly zero-day attacks come out even with all the defensive measures.

Some security researchers have pointed to the fact that autonomous vehicles can be hacked. For instance, Alexey Kurakin, Ian J. Good Fellow and Sami Bengio demonstrated how autonomous vehicles can be hacked by manipulating traffic signs to confuse the learning model.[31] Developments in ease of AI based malware and exploits will further complicate the security of autonomous platforms. An autonomous nuclear delivery platform can be compromised and made to launch an attack against the wrong country. Such a situation may pose a serious dilemma for the decision makers at all levels. Generally, it is believed that a pre-programmed UAV will reduce the risks of cyber-attack on communication lines.[32] The UAVs, however, can be hacked and identified by using electronic and digital jamming techniques. In June 2019, Iran identified and shot US surveillance monster (drone) RQ-4A Global Hawk. The drone was capable of conducting advanced recon and surveillance missions by using infrared, thermal imaging, radar, and electro-optical imaging.[33]

In addition, when such autonomous platforms are put under communication dead environment (pre-programmed), the operator and decision maker may not be able to detect that the system was not functioning properly. A malfunction in the system may jeopardize the whole operation. Likewise, a malfunctioned autonomous system may also launch four weapons instead of one. These scenarios will not only bring key challenges to the cybersecurity of these systems, but they will also add complexity to the reliability of their command and control system.

The impact of AI on nuclear doctrines

The use of autonomous delivery platforms and autonomous detection systems will increase the time urgency and pose several risks to the second strike capability of the states with less AI capabilities. This will compel states to rely on comparatively more ready nuclear arsenal where weapons are placed close to the delivery systems. The less AI capable states may also delegate the authority to use these weapons to lower commanders owing to the time urgent decision making needs. These states may decide to increase the number of their nuclear warheads to ensure survival of a sufficient number of their weapons in an attack situation. Time urgent nuclear doctrines will also be more prone to accidental and unauthorized nuclear launch. However, on the other hand, states with superior AI based detection systems may resort to first strike doctrines, though for different reasons. They might become confident to destroy their enemy in a comprehensive first strike and intercept the remaining retaliatory enemy strike by the timely identification of their AI based detection systems and leaving their missile defences to do the remaining job.

The dangers of AI swarms

The possibilities of terrorists getting their hands on dirty bombs and autonomous platforms are all real. [34] The detection technology is still not able to develop a reliable solution to deal with the problem, and counterterrorism officials are still facing problems to cooperate and coordinate their efforts at all levels.[35] For instance, it would be difficult to counter a hundred thousand drones carrying dozens of dirty bombs. How would an aircraft formation respond or neutralize such a threat? Imagine if a swarm of undersea drones launches an attack on the naval fleet, or is used in the detection of submarines underwater. Further studies would be needed to assess the impact of such technologies on nuclear deterrence stability.

These swarms can bring significant advantage to the navy, air force, army and nuclear forces of any nation. The software once written can be copied and distributed all over the world. In addition, mini drones are now becoming cheaper, more efficient, and easily available. Not only that the terror group ISIS has actually operated flying drones to conduct an IED attack, but it was also used for an assassination attempt on Venezuelan President Nicolas Maduro.[36] Therefore, with the inception of AI hardware and software agents, the threat of the use of dirty bombs by terrorists has increased.

The ethics of using AI in nuclear matters

The possibility of using AI in nuclear matters would raise several key ethical issues. For instance, if an AI-robot launches nuclear weapons in an unintended situation, who would own the destruction and causalities? Another issue is the occurrence of algorithmic decisions based on large, but not necessarily accurate data sets.[37] The biased data input could affect the decisions to launch nuclear weapons, which could lead to a crisis.

Conclusion

The rise in the malicious use of AI may increase the risk of accidents, nuclear war, and escalation. The ease of exploit development, AI spoofing, and the range of advanced tools will allow hackers to compromise more computers and networks, and the use of AI in nuclear affairs will bring aggressive nuclear doctrines.

States with less AI capabilities may resort to nuclear first strike or use cyber offence as protective measures. However, the cyber offence as a countermeasure is a mixed blessing. It could be dangerous if used to divert the attack on the wrong country.

In addition, the state with advanced AI capabilities may also like to opt counterforce first strike based on the accurate and more reliable information received by its autonomous detection systems. However, some of the enemy weapons may survive and the adversary may launch them against unguarded heavily populated cities.

The autonomous delivery platforms are also vulnerable to cyberattacks, as, like all other computer-driven systems, they run on software, and every software is vulnerable to cyber attacks and particularly to zero-day attacks.

There is a possibility of terrorists using cheaper and more effective autonomous drones, to conduct attacks on nuclear facilities of a country. For instance, an aircraft or a battle carrier group cannot neutralize a swarm of a thousand drones that can fly 1500 miles at the speed of 60m/h. Some states may even have the ability to use millions of such drones coupled with other technologies in a battlefield.

Although, the malicious use of AI will allow for more targets for hacking, however, it can help auto-detect the existing vulnerabilities and misconfigurations in the autonomous systems, AI based platforms, networks, and computers before an attacker could compromise it. In 2016, the US defense advanced research projects agency (DARPA) practically demonstrated the use of autonomous computers, which detected software flaws, and implemented patches to fix the bugs.[38]

The autonomous agent not only can predict the type and nature of future attacks but may also help in tracing the attacker by comparing the attack signatures with the existing database. It cannot only help identify the unknown programs but will also help in tracking them down. Another possibility is the use of autonomous software that can identify the flaws in the software of autonomous systems by frequent pen testing. This will issue a premature warning about the vulnerabilities and the time to fix them before the adversary in the real time operations succeeds in exploiting it. In addition, the intrusion detection system (IDS) specially designed to meet the requirement and needs of autonomous platforms would be helpful in determining malicious intrusions in real time operations. For instance, an autonomous vehicle can be programmed to stop all of its operations if the IDS issues an intrusion warning. However, quantum computing and AI based cryptanalyst tools may be a key challenge to secure strategic communications.

Spoofing early warning systems could cause an inadvertent escalation. For instance, what if malicious actors hack into early warning systems and trigger a false alarm. This could start an unintended nuclear war. The AI based decision making, however, could be useful in making sense of big data, time urgent responses in a stressful environment. At the same time, it has some serious ethical and reliability issues.

Endnotes

[1] For discussion about revolution in remote sensing and precision targeting see, Keir A. Leiber, and Daryl G. Press, "The new era of counterforce: Technological change and future of nuclear deterrence," *International Security* 41, no.2 (Spring 2017): 9-11.

[2] Horowitz, M. C., "When speed kills: autonomous weapon systems, deterrence, and stability," Working paper, University of Pennsylvania, Apr. 2019.

[3] Dr. Michael J. Garbade, “Clearing the confusion: AI vs Machine learning vs Deep learning Differences,” Towards Data Science, accessed Oct 17, 2019, https://towardsdatascience.com/clearing-the-confusion-ai-vs-machine-learning-vs-deep-learning-differences-fce69b21d5eb

[4] Ibid.

[5] Paul Sciglar, “What is Artificial Intelligence? Understanding 3 Basic AI Concepts,” Robotics Business Review, accessed Dec 31, 2018, https://www.roboticsbusinessreview.com/ai/3-basic-ai-concepts-explain-artificial-intelligence/

[6] Daniel S. Hoadley, and Nathan J. Lucas, “Artificial Intelligence and National Security,” *Congressional Research Service* (April 2018): 1

[7] William Carter, etal. “A National Machine Intelligence Strategy for the United States,” *CSIS* (March 2018) 1.

[8]“Artificial Intelligence and Machine learning made simple,” Maruti labs, accessed Dec 31, 2018, https://www.marutitech.com/artificial-intelligence-and-machine-learning/

[9] R. E. Uhrig and M. T. Buenaflor, “Artificial Intelligence and Training of Nuclear Reactor Personnel,” International OECD-CNSI Specialist Meeting on Training of Nuclear Reactor Personnel, Orlando, FL, accessed Oct 17, 2019, https://link.springer.com/chapter/10.1007/978-1-4613-1009-9_2.

[10] Nicole Kobie, “To cripple AI, hackers are turning data against itself,” Wired, accessed Oct 17, 2019, https://www.wired.co.uk/article/artificial-intelligence-hacking-machine-learning-adversarial

[11] Anirban Chakraborty, Manar Alam etal., “Adversarial Attacks and Defences: A survey,” Cornell University, accessed Sep 6, 2019, 4-5, https://arxiv.org/abs/1810.00069.

[12] Ilja Moisejev, “Evasion attacks on Machine Learning (or Adversarial Examples),” Towards Data Science, accessed July 21, 2019, https://towardsdatascience.com/evasion-attacks-on-machine-learning-or-adversarial-examples-12f2283e06a1

[13] Anirban Chakraborty etal., 5.

[14] Ibid.

[15] Ilja Moisejev, “Poisoning attacks on machine learning,” Towards Data Science, accessed Feb 05, 2019, https://towardsdatascience.com/poisoning-attacks-on-machine-learning-1ff247c254db

[16] Daniel Shapiro, “Artificial Intelligence and bad data,” Towards Data Science, accessed Oct 5, 2018, https://towardsdatascience.com/artificial-intelligence-and-bad-data-fbf2564c541a

[17] Mathew Green, “The Air force is developing an AI fighter,” Engineering.com, accessed Oct 2019, https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/18845/The-Air-Force-Is-Developing-an-AI-Fighter-Pilot.aspx

[18] “*Fuzzy classification trees* is a new model that integrates the fuzzy classifiers with decision trees, that can work well in classifying the data with noise. Instead of determining a single class for any

given instance, fuzzy classification predicts the degree of *possibility* for every class." Accessed at https://www.sciencedirect.com/science/article/pii/S0165011401002123

[19] Elad Kivelevitch, "AI system defeats expert human pilot," Aerospace America, accessed Sep 2019, https://aerospaceamerica.aiaa.org/year-in-review/ai-system-defeats-expert-human-pilot/

[20] Jaganath Sankaran, "A different use for artificial intelligence in nuclear weapons command and control," War on Rocks, accessed Feb 2019, https://warontherocks.com/2019/04/a-different-use-for-artificial-intelligence-in-nuclear-weapons-command-and-control/

[21] Michael C. Horowitz, "Artificial Intelligence and Nuclear Stability." in ed. Vincent Boulanin, *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk* (Stockholm International Peace Research Institute, May 2019), 81-83.

[22] Matt field, "Strangelov redux: US experts propose having AI control nuclear weapons," https://thebulletin.org/2019/08/strangelove-redux-us-experts-propose-having-ai-control-nuclear-weapons/

[23] Richard A. Best Jr. etal. "Intelligence, Surveillance, Reconnaissance (ISR) programs: Issues for Congress," CRS Report for Congress, accessed Aug 2019, https://fas.org/sgp/crs/intel/RL32508.pdf

[24] "How Artificial Intelligence Could increase the Risk of Nuclear War," RAND, accessed Oct 2018, https://www.rand.org/blog/articles/2018/04/how-artificial-intelligence-could-increase-the-risk.html

[25] Dr. Thomas Killion, "Transforming ISR capabilities through AI, machine learning and big data," Disruptive Technology for Defence Transformation, accessed Oct 2019, https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data

[26] Syed Sadam Hussain Shah, "Offensive Cyber Operations and Nuclear Weapons," CSIS, accessed Aug 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/190313_Shah_OffensiveCyber_pageproofs2.pdf

[27] John Seymour, and Philip Tully, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter," Black Hat, accessed Sep 2019, https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf

[28] George Dvorsky, "Hackers Have Already Started to Weaponize Artificial Intelligence," Gizmodo, accessed Aug 2019, https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425

[29] Ariel Conn, "AI and Nuclear Weapons – Trust, Accidents, and New Risks with Paul Scharre and Mike Horowitz," Future of Life, accessed March 2019, https://futureoflife.org/2018/09/27/podcast-ai-and-nuclear-weapons-trust-accidents-and-new-risks-with-paul-scharre-and-mike-horowitz/

[30] "The weaponization of increasingly autonomous technologies: Autonomous weapons systems and cyber operations," UNIDIR, accessed Nov 2018, 9,

https://unidir.org/files/publications/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf

[31] Anirban Chakrabortay, etal. 1-4.

[32] Michael C. Horowitz, "Artificial Intelligence and Nuclear Stability," 81.

[33] Lily Hay Newman, "The drone Iran shot down was a $220 M surveillance monster," accessed Aug 2019, https://www.wired.com/story/iran-global-hawk-drone-surveillance/

[34] "Dirty bomb what you should know," Environmental Protection Agency, accessed Feb 2019, http://www.epa.ie/radiation/emerg/mef/bombs/

[35] Pamela S. Falk, "The Dirty Bomb Threat," Foreign Affairs, accessed July 2019, https://www.foreignaffairs.com/articles/2017-04-04/dirty-bomb-threat

[36] Snyder J. Freedberg Jr. "Genocide Swarms & Assassin Drones: The Case For Banning Lethal AI," Breaking Defence, accessed Dec 2018, https://breakingdefense.com/2019/03/genocide-swarms-assassin-drones-the-case-for-banning-lethal-ai/

[37] Patrick Tucker, "Pentagon seeks a list of ethical principles for use of AI in War," Defence One, accessed Sep 2019, https://www.defenseone.com/technology/2019/1/pentagon-seeks-list-ethical-es-using-ai-war/153940/

[38] Michael Sulmeyer, "Beyond killer robots: How artificial intelligence can improve resilience in cyber space," Belfer Center for Science and International Security, Harvard University, accessed Aug 2019, https://www.belfercenter.org/publication/beyond-killer-robots-how-artificial-intelligence-can-improve-resilience-cyber-space