Artificial Intelligence and International Security: The Long View

*Amandeep Singh Gill**

War planners have always searched for tools that offer speed, accuracy, and the tailoring of force to the objective at hand. What if a technology could be found to deliver firepower at machine speed with 100 percent accuracy and enable commanders to modify force in real time to meet the political objectives set for a conflict? And, importantly for politicians, what if in pursuing these goals the only risk was mangled metal and fried computers? This is what artificial intelligence (AI) or, more accurately, autonomous and intelligent systems promise to deliver for military planners.[1] For nations faced with demographic decline and rich populations averse to conflict, the prospect of wars without body bags is indeed hugely attractive.

This essay argues that AI will have an impact on the conduct of warfare, bring new capabilities into being, and alter power equations. It will challenge traditional arms control thinking and raise questions about compliance with international law. New tools and competences will be required, and inventive ways to build trust and confidence among users will be needed. While binding norms will eventually be necessary to manage AI's international security implications, a good start can be made through a principles and standards–driven approach to governance. The growing civilian applications of AI offer an opportunity to build a tiered, multistakeholder governance toolkit.

Is AI a Game Changer in Combat?

An important question arises at the outset. To what extent do AI-enabled weapons constitute a break from the past? After all, means of delivering lethal force

*The views expressed in this article are the author's own.

Ethics & International Affairs, 33, no. 2 (2019), pp. 169–179.

doi:10.1017/S0892679419000145

remotely and automatically have been around for decades, among them the Tomahawk series of cruise missiles, the joint air-to-surface standoff missile, and tactical air defense systems such as the Phalanx Close-In Weapon System.[2] More recently, armed drones have been used in loitering mode in remote theaters for counterterrorism operations. Computerized decision support systems and simulators for training have been around for a long while; and algorithms that crunch data from multiple sources are a staple in advanced conventional weaponry, such as fighter jets.

With the introduction of AI techniques such as machine learning, deep neural networks, and reinforcement learning, there has been a shift from rule-based deterministic systems to more data-driven and outcome-oriented systems. AI-enabled machines can extract insights from training data in ways that are not always apparent to human programmers, and during operations they can handle much more data volume than traditional systems. For example, the U.S. Department of Defense's Project Maven can accelerate the processing of huge volumes of video footage coming in from drones to allow better target acquisition. Further, such computing can happen closer to the front lines where the combat is taking place, eliminating the need to transmit data on vulnerable high-bandwidth channels back to home base. Once we start to introduce AI into conventional weapons systems, a number of previously intractable problems, such as the hunting of nuclear submarines in the depths of the oceans, begin to appear solvable. New ways of delivering force—say, through swarms of unmanned aerial or underwater vehicles—also become feasible.[3] Of course, it is not all about high-level effects; some of the dirty, dangerous, and dreary tasks of the foot soldier may also begin to be handed over to autonomous systems.

It is perhaps unlikely that two decades from now wars will be fought between armies of robots, fleets of ghost ships, and packs of unmanned aerial vehicles (UAVs), but it is certain that combat systems will have much more autonomy and humans will be working much more closely with machines than they do today. This trend is in line with what is visible today on the civilian side, where what is called "narrow AI"—that is, algorithms suited to a single specific task—is emerging in diverse applications even as research is expanding in the area of "broad AI." As battle spaces expand to cover the globe, as the speed of engagement accelerates, and as peer powers compete in information-degraded battle environments thousands of miles away from the home base, autonomy—intelligent autonomy in particular—will rise in salience. This will be reflected in areas

such as autonomous surveillance and combat systems, adaptive communication systems, cyberattack mitigation and counterattack systems, and decision-making systems that depend on multisensor data fusion.[4] Technology has been a handmaiden to war since the beginning of history, but what could eventually set AI-enabled weapons apart is the prospect of losing human control.[5]

AI's Broader Geopolitical Impact

While AI may reshape how wars are fought and won, the geopolitical stakes are much broader. As important as military competition is the struggle for an economic edge, as advanced economies try to squeeze out every extra percentage point of GDP growth and as emerging economies attempt to catch up by harnessing leapfrogging technologies. There is no other sector, with the exception perhaps of the cyber domain, where the commercial stakes are so high and so intertwined with the security stakes. If we look at the top countries with relevant capabilities—Canada, China, France, Germany, India, Israel, Japan, Russia, South Korea, the United Kingdom, and the United States—we see this entanglement at work. Eight of these eleven are in the Asia-Pacific region (if you include Canada and the United States, given their Pacific coasts), which is rife with security dilemmas, and all but Israel are members of the G20.

Indeed, the competition to reap the security and economic benefits from AI might be highest between China and the United States. If data, entrepreneurial flair, state investments, and computing capacity are what matter most for a future in which AI plays a major role, it is hard to refute the argument that AI will end up increasing the gap in military and economic clout between these two countries and the rest of the world. However, this is not written in stone. The future of AI could rely on less-data-hungry techniques and new ways of combining cyber and physical capabilities. This might level the playing field for actors such as Europe, Canada, and Japan. AI expansion could also be fueled by digital public goods and the application of AI to development problems at scale, giving India an advantage because of the combination of a billion digital identities, half a billion smartphone users, and a similar number of new participants in digital payment systems.[6] Smart regulation and social trust could also create a competitive edge for certain regions provided that trained human resources are available in the right entrepreneurial environment to seize the opportunity. This seems to be the calculation in the European Union.

Putting a figure on the degree to which AI will catalyze the growth of comprehensive national power might be impossible.[7] But while think tanks have been cautious, consultants have taken the leap. Based on research from June 2017 to December 2017, the consulting firm Accenture estimates that AI could double annual economic growth rates in twelve developed economies by 2035, compared to a baseline scenario where AI has not been absorbed into the economy.[8] Another consulting firm, PwC, estimates that AI will add $15.7 trillion to world GDP by 2030, with the biggest global impact (almost 70 percent of the total) in just two geographies: China ($7 trillion) and North America ($3.7 trillion).[9] While AI is unlikely to radically change the economic sweepstakes in the middle of the twenty-first century, when China, the United States, and India are expected to be the largest economies, it could affect the pace of the shift and relative power differentials among the major players.

For comparison, we can look back at the trajectory of the Internet as an enabling technology for economic growth and geopolitical dominance. In the mid-1980s when domain name servers started to go up, no one could have predicted the eventual and current dominance of e-commerce.[10] Nor could anyone have predicted that countries such as China and Israel would develop formidable cyber warfare capabilities, giving them a competitive edge over their adversaries. Similarly, it is hard to predict how AI technologies will shape the power equations in the coming decades, particularly given the amorphous, distributed, and context-specific nature of their use. It is safe to say, however, that states with advanced data economies, sophisticated risk capital ecosystems, large research and development investments, and human resource capacities will have the first-mover advantage in boosting economic output through AI. And states currently dominant in advanced conventional weaponry and information and communication technology will accrue power through greater use of autonomous and intelligent systems. Those states left behind might seek to level the playing field through asymmetric responses using "old-fashioned" weapons of mass destruction or newer forms of disruption aimed at the increased vulnerabilities that have arisen with the Internet of Things.[11] These include cyber warfare and digital manipulation of public opinion. AI may also turbocharge cyber weapons by giving them the capability to adapt in real time to the changing tactics and tools of the defenders, and by facilitating deep fakes and targeted attacks customized by users.[12]

Even before a single shot has been fired by a machine in anger, AI has already begun to have implications for international security. The first casualty in the

struggle for AI dominance has been mutual trust. U.S. analysts have pointed to China's July 2017 Next Generation Artificial Intelligence Development Plan, which notes the historic opportunity offered by AI to leapfrog in national security technologies as evidence of Chinese plans to use AI to aggressively enhance national competitiveness.[13] These analysts also point to the rapid emergence of world-class Chinese AI companies, such as SenseTime (specializing in computer vision and deep learning) and DJI (specializing in UAVs), as evidence of China catching up with the United States, which some argue is overinvested in mature technologies and underinvested in disruptive breakthroughs. Also figuring prominently in these debates are Chinese investments in 5G—the low-latency, high-bandwidth telecom networks critical to the next generation of cyber physical systems—which might include AI-powered military systems.[14] The public discourse is often evocative of the crisis of confidence in the West triggered by the Soviet Union's launch of the Sputnik satellite in the early years of the Cold War, which would come to be seen as the start of the space race.

The impression of a similar incipient "race" is hard to avoid with even a cursory look at high-level statements and initiatives. Russian president Vladimir Putin, for example, told students at the beginning of the 2017 academic year that "whoever becomes the leader in [AI] will become the ruler of the world."[15] In March 2018, French president Emmanuel Macron announced that the country would make a five-year €1.5 billion investment in AI to start to catch up with China and the United States and "recreate a European sovereignty in AI."[16] And in the home of laissez-faire, free-wheeling tech capitalism, U.S. president Donald Trump signed an executive order in February 2019 entitled Maintaining American Leadership in Artificial Intelligence. The order deems AI of "paramount importance to maintaining the economic and national security of the United States" and calls for AI breakthroughs to be rapidly transitioned into "capabilities that contribute to our economic and national security."[17] The order follows the creation by the Pentagon of the Joint Artificial Intelligence Center in June 2018 as a focal point to harness the potential of AI to transform all functions of the U.S. Department of Defense.[18]

The Challenge to Traditional Arms Control

From an arms control perspective, the central questions are whether AI in weapons systems would lower the threshold for the use of force in international relations,

whether it would accentuate strategic instability, and whether it would trigger new arms races and empower shadowy nonstate actors. The answers are not simple, as they were not during the Cold War when analysts debated whether a particular strategic weapon system upheld or undermined first-strike stability, crisis stability, and the offense-defense equation. For example, depending on your perspective, adding AI capabilities to hypersonic glide vehicles such as China's DF-ZF could undermine strategic stability or could restore stable deterrence by helping pierce an opponent's missile defense systems.[19] Autonomous swarms of UAVs could bolster defense by defending battleship groups exercising freedom of navigation or they could ease offense by degrading an opponent's forward maritime defense strategy. Shifting capabilities in combat to the "edge"—where data is being generated and rapid computing responses are required—could reduce the vulnerability of far-flung forces to surprise attack or it could make war termination more difficult. Use of autonomous weapons against a predominantly human rebel force could bring stability quickly to an ungoverned space or it could be used to justify asymmetric attacks against civilians and digital infrastructure.[20]

As in the Cold War years, the answers to these questions may lie in a combination of responsible doctrines, command and control, confidence building and dialogue, agreed measures for restraint, and a patient buildup of shared norms. Further, the answers will likely need to be tweaked iteratively as lessons are learned through less-than-catastrophic failures. But the toolkit of arms control and the mindsets of practitioners will have to evolve.[21]

Disarmament and arms control specialists are accustomed to dealing with tanks, aircraft, and missiles—not data and algorithms. And they are used to negotiating at a leisurely pace with those who share their paradigm.[22] The outcomes they seek mostly involve hard law and intrusive verification regimes. Autonomous and intelligent systems, by contrast, are not well suited to such forms of arms control. Lethal autonomy is not so much about discrete, countable systems as it is about the penetration of AI into weapons capabilities. The technology landscape seems to shift about every six months and thus does not lend itself to rigid normative frameworks. Verifying training data sets and algorithms to ensure compliance with agreed-upon rules on lethal autonomy poses unique challenges compared to verifying production pathways to nuclear or chemical weapons.[23] And even more than in the case of nuclear and space capabilities, intellectual property and cutting-edge human resources rest with the private

sector, which does not participate in current forums on disarmament, international security, and arms control.[24]

An Agenda For Ensuring Security and Stability in the Age of AI

The starting point for dealing with the international security implications of AI must be the acknowledgment that we are in it for the long haul. There will be no quick fixes. The economic, political, and security drivers for mainstreaming this suite of technologies into security functions are simply too powerful to be rolled back. There will be plenty of persuasive national security applications—minimizing casualties and collateral damage through better discrimination of targets, fighting crime, defeating terrorist threats, saving on defense spending, and protecting soldiers and their bases—to provide counterarguments against concerns about runaway robots or accidental war caused by machine error.

This acknowledgment must be accompanied by an intensification of cross-domain literacy. AI cannot be the business of coders and cognitive scientists alone; nor can its security implications be the province only of diplomats, generals, and lawyers. Given the broad impact that AI businesses can have on society, the business of AI has to be everyone's business. Governance of AI can only be based on a correct understanding of the power and limits of the technology, and such governance can only be effective globally if it is part of a tiered approach that includes actors at the intergovernmental, national, and industry levels.

Currently, though military investments in AI are being acknowledged, no state admits to the existence of lethal autonomous weapon systems in its inventory.[25] Thus, if we want to build mutual confidence and trust, we are left either to add discussions on such systems to existing dialogues on cybersecurity and arms control more broadly or to begin with new dialogues on approaches to repurposable civilian capabilities. The latter might be a more productive venue for engaging the private sector, which is wary of being stigmatized by civil society as the maker or facilitator of "killer robots." Tagging on discussions of AI to cybersecurity or traditional arms control would also be unhelpful because of the risk of false analogies.[26]

Thus, new innovatively structured dialogues in the track 1.5 setting (involving both government and nongovernmental parties) or the track 2 setting (involving

only informal nongovernmental parties) are required. The first objective should be to enhance mutual understanding through in-depth discussions on national approaches to AI development, testing and validation, deployment, and use. Another objective should be to allow some sharing of best practices or cautionary experiences.[27] A third potential objective would be to shift thinking from zero-sum competitive approaches to collaborative problem-solving using data and algorithmic insights pooled by the participants themselves or put in escrow with a trusted third party.

Agreement on norms to govern the military use of AI could take time, but influencing the direction of such use by other means brooks no delay. One important channel for shaping AI use globally is guiding principles short of binding law. At a time when there are trust deficits among nations and multilateral negotiations are at best seen as opportunities for "lawfare," it makes sense to rally around shared values and ethical principles. In the context of emerging technologies, such an approach also permits more of an impact early on in the innovation cycle, when national or international regulatory reach is absent or ambiguous. Consistent with this logic, the EU High-Level Expert Group on Artificial Intelligence has identified five principles—beneficence, nonmaleficence, autonomy of humans, justice, and explicability—for the trustworthy and ethical development of AI.[28]

More specifically, in the context of military use, in 2018 the Group of Governmental Experts of the Convention on Certain Conventional Weapons on emerging technologies in the area of lethal autonomous weapon systems (LAWS), comprised of 125 states and including all countries thought to be pursuing national security applications of AI, identified ten guiding principles on emerging technologies in the area of LAWS. These principles cover aspects related to the applicability of international humanitarian law, human responsibility, accountability, risk assessment and mitigation, and the need to take a nonanthropomorphic view of such systems. The guiding principles are accompanied by building blocks of common understandings on definitions and the nature of human intervention required throughout the various stages of technology development and deployment to uphold compliance with international law, in particular international humanitarian law.[29]

Another channel for the soft governance of AI could be engineering standards and codes. At a minimum, a common vocabulary for assessing risks and aligning design with safety and reliability considerations is needed. The Institute of

Electrical and Electronics Engineers' Global Initiative on Ethics of Autonomous and Intelligent Systems has started building a shared, multidisciplinary, and evolving resource of terms.[30] There is further scope for constructing common standards that can progressively align practices around the globe to responsible principles.

Last Word

There is a growing concern over the repurposing of AI technologies for warfare.[31] As with cyber weapons, LAWS could have indiscriminate effects and be turned around to attack the attackers.[32] They can create challenges for the application of international humanitarian law principles, such as distinction, proportionality, and precaution, all of which presuppose a degree of human reflection and control. Their international security implications are still unfolding but could be as significant as the nuclear revolution in warfare, if not more so. Innovative and agile ways of governing the use of AI are needed urgently to head off risks to international peace and security.

NOTES

[1] The term "autonomous and intelligent systems" follows the practice of the Institute of Electrical and Electronics Engineers. The sense conveyed is that of augmentation of human capabilities, and not of their emulation.

[2] For a full listing, see Neil Davison and Gilles Giacca, "Part III: Background Paper Prepared by the International Committee of the Red Cross," in *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons* (meeting report, International Committee of the Red Cross, Versoix, Switzerland, March 15–16, 2016), pp. 69–84, shop.icrc.org/autonomous-weapons-systems.html.

[3] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton, 2018), pp. 11–13.

[4] *Report of the Artificial Intelligence Task Force*, Government of India, Ministry of Commerce and Industry, dipp.gov.in/whats-new/report-task-force-artificial-intelligence.

[5] Amandeep S. Gill, introduction to *Perspectives on Lethal Autonomous Weapon Systems*, UNODA Occasional Papers 30, November 2017, pp. 1–4, s3.amazonaws.com/unoda-web/wp-content/uploads/2017/11/op30.pdf.

[6] Ananya Bhattacharya, "The Number of Smart Phone Users Will More Than Double in Four Years," Quartz India, December 4, 2018, qz.com/india/1483368/indias-smartphone-internet-usage-will-surge-by-2022-cisco-says/; and Kiran Rathee, "How Digitally Enabled Government Saved Rs 90,000 Crore," *Financial Express*, February 2, 2019, www.financialexpress.com/industry/technology/how-digitally-enabled-government-saved-rs-90000-crore/1472379/.

[7] Chinese scholars use the term *zonghe guoli* (comprehensive national power) to refer to an aggregate of factors such as territory, availability of natural resources, military strength, economic clout, social conditions, domestic government, foreign policy, and other forms of wielding international influence. See Michael Pillsbury, *China Debates the Future Security Environment* (Washington, D.C.: National Defense University Press, 2000), pp. 203–4.

[8] Mark Purdy and Paul Daugherty, *How AI Boosts Industry Profits and Innovation*, Accenture, www.accenture.com/_acnmedia/Accenture/next-gen-5/insight-ai-industry-growth/pdf/Accenture-AI-Industry-Growth-Full-Report.pdf?la=en.

[9] PwC, *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise?* available at www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

[10] See Longmei Zhang and Sally Chen, "China's Digital Economy: Opportunities and Risks" (working paper 19/16, Asia Pacific Department, International Monetary Fund, January 2019), www.imf.org/~/media/Files/Publications/WP/2019/wp1916.ashx.

[11] For an idea of the number of devices that are part of the Internet of Things, see Knud Lasse Lueth, "State of the IoT 2018: Number of IoT Devices Now at 7B—Market Accelerating," IoT Analytics, August 8, 2018, iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/; Japan's National Institute of Information and Communications Technology (NICT) estimates on the basis of scans of the Darknet that 54 percent of the attacks it detected in 2017 targeted Internet of Things devices.

[12] For example, IBM researchers managed to conceal the known malware WannaCry in video-conferencing software and use an AI neural network to trigger it in response to use by a specific individual. See Mark Ph. Stoecklin, "DeepLocker: How AI Can Power a Stealthy New Breed of Malware," SecurityIntelligence, August 8, 2018, securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/.

[13] Translated text of the Plan available on the website of the Chinese Embassy in Finland: http://www.chinaembassy-fi.org/eng/kxjs/P020171025789108009001.pdf. For a reaction, see Gregory C. Allen, "Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," Center for a New American Security, February 6, 2019, www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

[14] John Gapper, "Huawei Is Too Great a Security Gamble for 5G Networks," *Financial Times*, January 30, 2019, www.ft.com/content/40e68898-23b8-11e9-8ce6-5db4543da632.

[15] Vladimir Putin, quoted in "'Whoever Leads in AI Will Rule the World': Putin to Russian Children on Knowledge Day," RT, September 1, 2017, www.rt.com/news/401731-ai-rule-world-putin/.

[16] Emmanuel Macron, quoted in Nicholas Thompson, "Emmanuel Macron Talks to WIRED about France's AI Strategy," *WIRED*, March 31, 2018, www.wired.com/story/emmanuel-macron-talks-to-wired-about-frances-ai-strategy/.

[17] "Executive Order on Maintaining American Leadership in Artificial Intelligence" (transcription of executive order, signed by Donald J. Trump, February 11, 2019), WhiteHouse.gov, www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[18] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity*, Defense.gov, media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[19] Lora Saalman, "Fear of False Negatives: AI and China's Nuclear Posture," Bulletin of the Atomic Scientists, April 24, 2018, thebulletin.org/2018/04/fear-of-false-negatives-ai-and-chinas-nuclear-posture/.

[20] Jai Galliott, *Military Robots: Mapping the Moral Landscape* (Burlington, Vt.: Ashgate, 2015), pp. 165–86.

[21] Remarks taken from Amandeep Singh Gill (SIPRI workshop, "Mapping the Impact of Machine Learning and Autonomy on Strategic Stability and Nuclear Risk," Stockholm, May 22–23, 2018).

[22] The arms control epistemic community is relatively closed; in contrast, other processes, such as the sherpas preparing for the Nuclear Security Summit, have been an experiment in opening up the community to other domain specialists. See Emanuel Adler, "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control," *International Organization* 46, no. 1 (winter 1992), pp. 101–45.

[23] Conversely, AI could bolster and radically reduce the costs of traditional verification methods.

[24] Except that the tech industry and its employees may be given a head start on these forums with an early vote on how military applications are pursued. The previously cited Project Maven triggered a controversy among Google employees. See Kelsey D. Atherton, "Targeting the Future of the DoD's Controversial Project Maven Initiative," C4ISRNET, July 27, 2018, www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/.

[25] See the official statements made by individual countries at a series of meetings held in in Geneva, at "2018 Group of Governmental Experts on Lethal Autonomous Weapon Systems," under "Statements," United Nations Office at Geneva, www.unog.ch/80256EE600585943/(http://Pages)/7C335E71DFCB29D1C1258243003E8724?OpenDocument.

[26] Two such false analogies from the author's experience come in the question of whether existing international law, in particular international humanitarian law, applies to cyber conflict, involving a bane of discussions on cyber norms, or to analogizing nuclear stability to the cyber domain.

[27] Joseph S. Nye Jr. cites the story of how the idea of "permissive action links" for securing nuclear weapons was leaked in an informal dialogue to the Soviets to help spread a good practice on nuclear security. Joseph S. Nye Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* 41, no. 3 (summer 1987), pp. 371–402.

[28] *Draft: Ethics Guidelines for Trustworthy AI*, European Commission High-Level Expert Group on Artificial Intelligence, December 18, 2018, ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai.

[29] Group of Governmental Experts of the High Contracting Parties to the 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, *Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, October 23, 2018, p. 4, https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/CCW_GGE.1_2018_3_final.pdf.

[30] *A* Glossary *for Discussion of Ethics of Autonomous and Intelligent Systems, Version 1*, IEEE Standards Association, October 2017, standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/eadv2_glossary.pdf.

[31] António Guterres, "Remarks at 'Web Summit'" (speech, Web Summit, Lisbon, November 5, 2018), www.un.org/sg/en/content/sg/speeches/2018-11-05/remarks-web-summit.

[32] NotPetya, the ransomware that caused havoc in summer 2017 in the global supply chains of companies in fields as diverse as shipping, construction, pharmaceuticals, and food, used a penetration capability called EternalBlue that was allegedly developed by the National Security Agency in the United States but leaked in early 2017.

Abstract: How will emerging autonomous and intelligent systems affect the international landscape of power and coercion two decades from now? Will the world see a new set of artificial intelligence (AI) hegemons just as it saw a handful of nuclear powers for most of the twentieth century? Will autonomous weapon systems make conflict more likely or will states find ways to control proliferation and build deterrence, as they have done (fitfully) with nuclear weapons? And importantly, will multilateral forums find ways to engage the technology holders, states as well as industry, in norm setting and other forms of controlling the competition? The answers to these questions lie not only in the scope and spread of military applications of AI technologies but also in how pervasive their civilian applications will be. Just as civil nuclear energy and peaceful uses of outer space have cut into and often shaped discussions on nuclear weapons and missiles, the burgeoning uses of AI in consumer products and services, health, education, and public infrastructure will shape views on norm setting and arms control. New mechanisms for trust and confidence-building measures might be needed not only between China and the United States—the top competitors in comprehensive national strength today—but also among a larger group of AI players, including Canada, France, Germany, India, Israel, Japan, Russia, South Korea, and the United Kingdom.

Keywords: artificial intelligence, international security, lethal autonomous weapons, cyber warfare, international humanitarian law, economic competition, confidence building, arms control, guiding principles, governance