CONTROLLING THE MENACE OF HIGH-TECH WEAPONS: A NEW DIRECTION FOR ARMS CONTROL

Ryan R. Swan, J.D., M.Phil.
Visiting Researcher, Bonn International Center for Conversion
Doctoral Candidate, Rhenish Friedrich Wilhelm University of Bonn

Haig Hovaness, M.B.A.
Secretary, Peace Action Committee of the Green Party of the United States

Abstract

This paper describes the risks posed by the advent of software-based weaponry (SBW) and the novel challenges it raises for existing arms control architectures. It highlights the fundamental mismatch between the dynamic, persistent character of SBW advancement and the static, intermittent nature of prevailing arms control practices, and argues that a new arms control model is needed in order to keep pace with the rapidly evolving SBW threat. It introduces a preliminary sketch of a modernized arms control approach that better accounts for the realities of contemporary arms development.

Keywords: *arms control, arms race, high-tech weapons, emerging technologies*

I. Introduction

Development of a new generation of software-based weapons (SBW) is accelerating in the course of an intensifying international arms race, unrestrained by existing arms control arrangements. Advanced nations are systematically adapting breakthroughs in software-controlled microelectronics to embed machine intelligence in a broad range of weapons. The software-intensive nature of these weapons systems allows them to be modified as quickly as improved software becomes available, enabling not just basic weapon performance improvements, but the provision of entirely new capabilities, such as networked cooperative operation and autonomous functioning.

The unique characteristics of SBW threaten to destabilize strategic dynamics between advanced military nations, heightening the risk of runaway escalation scenarios, inadvertent conflict provocation and third-party hacking. While regulatory containment of the Pandora's Box of high-tech arms racing is desperately needed, prevailing arms control frameworks are ill-suited to the task. The lumbering arms control processes of today developed in response to previous generations of primarily hardware-based weapon systems with static capabilities limited by physical characteristics. These weapons took considerable time to develop, deploy and subsequently modify, allowing the parties to conclude arms control agreements at wide intervals, with confidence that they would have sufficient time to gauge and manage future risk. The protean character of modern SBW creates a fundamental challenge for the static, slow-moving nature of existing arms control frameworks and practices.

We argue that the old paradigm simply cannot keep pace with rapidly evolving SBW threats and that a new arms control model is needed – one that is modernized to account for the contemporary and future realities of SBW. We introduce a preliminary sketch of a new regulatory framework for weapon capabilities for which i) software is intrinsic to weapon functioning; and ii) this software is readily modifiable. These criteria cover a range of kinetic, electro-magnetic and purely digital weapons categories and, given the current high-tech trend, will likely come to cover most sub-nuclear weaponry in the future. Our proposed framework is substantively tailored to address contemporary risks and challenges, and structurally designed to remedy recurrent problems which have plagued arms control efforts to date.

II. SBW Risks

SBW technology is being deployed in a wide variety of military systems in ground, naval, airborne, orbital, and cyber weapons systems. Software is a critical component of modern military systems enabling surveillance, targeting and engagement of enemy forces. It provides the "intelligence" that greatly amplifies the power of modern weaponry. We briefly highlight current SBW development in space, autonomous and cyber weapons. In each of these categories, dangerous arms racing is under way in the absence of effective arms control.

i. *Space Weapons*

With the launch of the Sputnik satellite in 1957, military planners immediately grasped the potential for exploitation of satellite technology. Any nation mastering this technology could greatly expand its surveillance, communications and weapons delivery capabilities on a global scale. No part of the world would be out of reach of orbital platforms circling the planet. As the U.S. and Soviet Union raced ahead in developing and deploying military reconnaissance and communications satellites, the ominous possibility of putting nuclear bombs in orbit led to the 1967 Outer Space Treaty (OST) banning nuclear weapons in space.

The OST ban, however, was limited to nuclear weapons and weapons of mass destruction. Weapons intended to attack orbital assets were not prohibited by the treaty, and this has become an active field of development and deployment. Advances in microelectronics and computing power have enabled a variety of ground-based and space-based offensive weapons designed to disable or destroy satellites. Without software-enabled systems for tracking, targeting and engaging satellites, this weaponry would be infeasible. The cataloging of the array of space weapons technology under development is beyond the scope of this paper, but it should be noted that there is a broad range of projects, all of which are complex, software-intensive, highly classified, and costly.[1] These can be roughly grouped as follows:

- Ground-based
    - Missile anti-satellite (ASAT) capabilities
    - Directed energy ASATs
    - Tracking and targeting facilities
    - Command and control facilities
    - Launch and recovery complexes

- Space-based
    - Recoverable vehicles (space planes)
    - Satellite ASATs (kinetic, electromagnetic, directed energy)
    - Orbital reconnaissance
    - Anti-satellite countermeasures (Anti-ASATs)

A primary global security risk posed by space weapons, particularly ASATs, is that of conflict escalation to nuclear war. Because reconnaissance, early warning and military communications satellites are essential components of a nation’s nuclear deterrent capability, the destruction or substantial degradation of these facilities could be viewed as a precursor to a nuclear attack and could lead to a nuclear exchange, especially if there were an imbalance in the anti-satellite capabilities of the adversary powers.[2]

Beyond the escalatory threat, there is additional cause for concern based in physics. As orbital space becomes increasingly populated by satellites, there is a danger of a cascade of destruction resulting from the accidental or deliberate breakup of one or more satellites. The so-called Kessler Syndrome is the possible large-scale destruction of many satellites in the same orbital region resulting from the snowballing propagation of debris from multiple collisions. Although scientists assign a low probability to this outcome based on the predicted rate of accidental collisions, warfare involving the deliberate destruction of large numbers of satellites could significantly increase the odds of such a catastrophe.[3] The resulting loss of numerous civilian communications, weather and global positioning satellites could cause significant disruption to the world economy.

ii. Autonomous Weapons

The industrial revolution introduced the war machine as a major factor in armed conflict. By the mid-20th century, tanks, aircraft, submarines, and warships had become the decisive weapons of conventional war, but they were all directly operated by human occupants. The efficacy of these weapons was limited by the physical stamina, skill and motivation of the personnel controlling them. Today's unmanned combat vehicles will out-perform human operators in basic tasks requiring speed, accuracy and endurance.[4] Pilotless fighter jets can sustain high-G turns that would render a human pilot unconscious.[5] Robotic warships can reliably patrol vast areas, immune to fatigue.[6] The obvious advantages offered by computer control of mobile weapons have led to numerous substantial development programs in all major militaries. Examples include the following:

- Uran-9 combat vehicle (Russia)
- Skyborg unmanned combat aircraft (U.S. Air Force)
- Sea Hunter anti-submarine ship (U.S. Navy)
- X37 space plane (U.S. Space Command)

It is important to note that the capabilities of software-based robotic systems improve steadily as their software is updated and augmented, without requiring hardware changes. This novel characteristic poses serious challenges for arms control efforts because there is no visible evidence of a software-based weapon's altered characteristics. Moreover, almost any remotely operated robotic weapon system can be modified to become partially or fully autonomous with the addition of appropriate software and computing components, again without any visible alteration.

The issue of fully autonomous weapons is a crucial one for the preservation of world peace. Historically, humans have been responsible for acts of war. From the highest commander to the lowest rank of soldier, individual decisions have been linked to the resulting consequences. Although the fog of war often obscures this responsibility, it has been a fundamental assumption of politics and law. With the appearance of war machines that can independently decide when to kill, there is an epochal change in the nature of warfare. It may be argued that if humans remain in control of the engagement authority (decision to attack) of an automated weapon, then accountability can easily be preserved. Unfortunately, there is a powerful evolutionary force operating against this cautionary principle.

In the 1950s, the American military strategist John Boyd formulated a general theory of armed conflict based on a cyclic pattern called the OODA loop (Observe-Orient-Decide-Act). The key insight of this theory is that the combatant who can execute this loop faster than an adversary has an advantage because the adversary's reactions will lag the current state of the conflict, leading to incorrect actions. According to Boyd, speed of decision-making is the key to victory:

> "*The ability to operate at a faster tempo or rhythm than an adversary enables one to fold the adversary back inside himself so that he can neither appreciate*

> *nor keep up with what is going on. He will become disoriented and confused.*"[7]

This theory has been widely adopted and is reflected in the weapons development practices of all advanced nations. The application of OODA loop theory to combat involving autonomous weapons leads to the conclusion that the autonomous system should execute the loop at maximum speed, and this includes the "decision" step part of the loop. Thus, an autonomous weapons system requiring the delay of human approval for target engagement will be inferior to an adversary system that makes this decision automatically. Absent global conventions limiting the autonomy of lethal weaponry, there will be a steady trend toward granting engagement authority to such weapons.

If autonomous weapons are granted full engagement authority, two major problems arise: i) the danger of escalation and ii) the difficulty of assigning responsibility for inappropriate weapons use. Escalation danger arises from the interconnection of multiple autonomous systems acting in concert with lightning speed. The higher up the ladder of decision-making authority the automated systems climb, the greater the escalation risk, culminating in the realization of a nuclear doomsday machine. At every stage it will be argued that competitive advantage is gained by giving the automated systems more authority, but this trend will steadily raise the risk and magnitude of a dangerous runaway escalation in which events outpace the ability of leaders to halt hostilities.

The issue of accountability for the accidental, unplanned or inappropriate operation of autonomous weapons concerns the diffused responsibility for the creation and deployment of such systems. If the weapon independently decides to destroy a target or kill individuals, where does the responsibility lie? It can be argued that all persons in the chain from the weapon designer to the battlefield personnel deploying the weapon are partially accountable. Although automated weapons can make decisions at computer speed, their ability to decide in ambiguous circumstances is limited by the logic of their software. Thus, the burden of dealing with an ethically problematic battlefield situation shifts from a front-line soldier to the software developer writing the code controlling the autonomous weapon. It is difficult to imagine how software could deal adequately with hostage situations, misidentification of friendly forces or commingled hostile and civilian personnel. The presence of machine intelligence does not obviate moral quandaries.

iii. *Cyber Weapons*

Unlike the software-empowered weapons discussed above, cyber weapons are pure software, with no physical embodiment. Thus, they are invisible, deliverable almost instantly, and capable of replicating and spreading rapidly and extensively. Cyber weapons owe their potency to the increasing reliance on interconnected computers by all sectors of society. Any computer system, military or civilian, is a potential target for a cyber weapon. Cyber weapons operate by inserting manipulative or destructive code (malware) into an enemy computer system. This is usually done by exploiting weaknesses in widely installed commercial operating systems or by otherwise circumventing system security protections. Once inside a target system, the cyber weapon can strike immediately or lie dormant, awaiting remote or timed activation. Harmful effects of cyber weapons can include theft of information, erasure of data, halting of systems, and destruction of physical facilities controlled by the target software. The malware can be programmed to spread beyond the immediate target to attack other accessible targets.

Because the development of software weapons does not require costly resources or specialized facilities, unscrupulous independent computer hackers develop malware tools for sale in a black market for computer “exploits” that enable malware to penetrate target computer systems. The security agencies of nation states compete to purchase these software tools to add to their cyber weapon arsenals,[8] but criminal elements can also obtain access to malware through purchase or theft of cyber weapon code. Thus, cyber weapons pose a dual threat to peace: cyber-attacks conducted by governments and similar attacks carried out by criminals.

The ease of transmission of software makes the development of malware a hazardous undertaking for nation states because it is difficult to secure arsenals of cyber-weapons. In 2017,
Wikileaks began to publish a stolen archive of NSA malware tools called Vault 7. Soon afterward, a series of ransomware attacks utilizing these tools occurred.[9] The contents of Vault 7 included a component called “Marble Framework” which enabled the masking of NSA cyber-weapons to conceal their source, possibly by leaving misleading traces indicating of foreign origin. The inability of nation states to reliably secure cyber-weapons is a serious concern and an important reason to restrain development of such weaponry.

Beyond the threat that cyber-weapons pose to civilian infrastructure is the escalation danger resulting from cyberattacks on military facilities. Because the nuclear forces of major powers rely on computerized warning and command and control facilities, a cyberattack on these systems could precipitate a nuclear exchange. Indeed, a statement in the U.S. 2018 Nuclear Posture Review explicitly acknowledges this possibility.

> *“the president will have an expanding range of limited and graduated [nuclear] options to credibly deter Russian nuclear or non-nuclear strategic attacks, which could now include attacks against U.S. NC3 [Nuclear Command, Control, and Communications], in space and cyberspace”*[10]

Despite the evident dangers of cyber weapon development, the U.S. is pressing ahead with military investments in cyber-warfare.[11] The newly established U.S. Cyber Command includes offensive capabilities in its operational scope.[12] Russia, China and other advanced nations are proceeding with similar military cyber-weaponry efforts.[13]

Because the development and deployment of cyber-weapons is entirely unregulated by arms control, these weapons are an increasing threat to global peace, both from a military conflict perspective and because of endangerment of civilian infrastructure. Thousands of factories, power plants, water supplies, hospitals, and communications networks can be damaged or disrupted by military or criminal cyber-attacks. Thus, applying effective arms control to cyber-weaponry is a matter of high importance.

III. SBW Challenges for Arms Control

The disruptive characteristics of present SBW development – speed of modification, secrecy of design, functional anomalies, hacking susceptibility, displacement of human control, and escalation potential – raise serious challenges for arms control. Pivotal questions include:

- How can SBW arms racing be restrained?
- How can SBW arms control compliance be verified?
- How can SBW arms control compliance be enforced?
- How can non-combatants be protected from potential consequences of SBW?
- How can human control be assured?

The recognition that the prevailing approach to major power arms control is ill-suited to address these challenges is already becoming evident. German Foreign Minister, Heiko Maas, called on global leaders to "rethink" arms control in light of the technological advancements of weapons capabilities, organizing several conferences on this topic.[14] Still, the formulation of actual solutions remains in a stage of infancy.

One route considered has been the subsumption of autonomous SBW under the existing Convention on Conventional Weapons (CCW). In 2013, states parties to the CCW agreed on a mandate for lethal autonomous weapons systems (LAWS) "to discuss the questions related to emerging technologies in the areas of lethal autonomous weapons systems in the context of the objectives and purposes of the [CCW]."[15] A series of meetings of a Governmental Group of Experts (GGE) have taken place, though, at present, this group is still exploring "possible recommendations on options related to emerging technologies in the area of LAWS…"[16]

A coalition of non-governmental organizations, including Human Rights Watch and Amnesty International, under the banner of the Campaign to Stop Killer Robots has advanced a proposal for a preemptive ban on LAWS. The idea for such a convention has the backing of the Holy See and some 30 nations, including China, which supports banning the use of LAWS.[17] Both the CCW's GGE and the ban campaign, however, fail to account for the range of SBW. A specific ban on LAWS neglects the emerging gamut of artificial intelligence-facilitated and software-enhanced weapons capabilities falling below the capability threshold of full autonomy, not to mention those capability sets in the cyber realm.

Apart from China, the major players in the SBW arms race, including the U.S., Russia, United Kingdom, and Israel, oppose a ban on LAWS. While evincing little interest in contemplation of broader SBW arms control, the U.S. and Russia favor a "basic rules of the road" approach in the context of cyber warfare.[18] At the 2021 Geneva Summit, the U.S. and Russia set forth basic interests in which the other side should not infringe without an expected response and agreed to further talks.[19] Other efforts, such as the Tallinn Manual attempting to bring cyberattacks into a law of war framework, advance a norms-based approach of best practices for the use of cyber weapons. This manner of proceeding fails to provide for binding regulation in the cybersphere, while ignoring the issues and risks posed by SBW more broadly.

We contend that these fragmentary proposals are insufficient to control the risks of SBW and to stem wasteful arms racing in their development and deployment. None of the proposed initiatives addresses the fundamental mismatch between the dynamic, persistent character of the SBW threat and the static and intermittent nature of historical arms control practices.

IV. Sketch of a New Direction for Arms Control

We contend that a new arms control model requires i) new substantive regulations tailored to the practical threats and realities of contemporary SBW; and ii) new structural means of enforcing these regulations in a manner that is sufficiently adaptive to keep pace with constant technological advancement and sufficiently impactful to ensure compliance. We base this new regime on the legal foundation of the Geneva Conventions and the Nuremberg Principles, noting the precedent of liability and effective punishment set by the Nuremberg Trials and the International Military Tribunal for the Far East.

i. *Functional Parameters*

The new model we are preliminarily sketching would be effectuated by an international, legally binding treaty providing for the regulation of the following weapon types classified as SBW:

1. weapons for which software is intrinsic to functioning; and
2. for which this software is modifiable.

The regulatory scope of this treaty and liabilities contained therein would extend to the following:

1. nation state governments and their armed forces responsible for the deployment of SBW;
2. private sector entities responsible for the manufacture of SBW; and
3. individuals directly or indirectly responsible for the use of SBW.

ii. *Substantive Provisions*

This new model would include, inter alia, the following substantive regulations:

1. *Ban all forms of indiscriminate anti-personnel SBW.* Any automated weapon designed to target and injure or kill individuals irrespective of their combatant status would be prohibited. Examples of such weapons would be intelligent drone swarms or loitering munitions programmed to recognize human targets.

2. *Criminalize all SBW attacks on civilian infrastructure*. Use of cyberweapons designed to disrupt, damage, or destroy civil infrastructure, such as power plants, water supplies, hospitals, transportation, or emergency services would be banned and their use (and planned use) would provide for criminal liability.

3. *Ban strategically destabilizing SBW.* All types of anti-satellite weapons, which greatly increase the danger of nuclear war, would be prohibited. Other destabilizing strategic systems, such as automated launch-on-warning retaliatory systems, would also be tightly restricted or banned.

4. *Ban autonomous engagement mode for anti-personnel SBW.* Weapons designed to independently decide when to kill or injure individuals would be

banned. Independent decision is defined as the ability of a weapon to strike without direct human authorization.

5. *Prohibit trade in commercial software security exploits.* The sale or purchase of software methods for defeating computer security for destructive purposes would be banned. This prohibition would apply to all entities engaged in such commerce: national, corporate, or individual.

6. *Restrict automated escalation in SBW battle management systems*. The escalation of hostilities under software control, independent of human management, would be prohibited. In addition, a circuit-breaker function would be required in all automated battle management systems to prevent erroneous runaway escalation.

7. *Prohibit improper modification of regulated SBW.* Because software is easily modified, it would be prohibited to deliberately modify an SBW system to make it non-compliant with relevant restrictions.

8. *Require kill-switch function in all autonomous combat systems.* To prevent accidental or deliberate undesired operation of an autonomous SBW system, all such systems with must incorporate a "kill-switch" permitting immediate remote deactivation of the autonomous mode.

iii. Structural Framework

The above enumerated provisions, though more comprehensive, are not so different from what might be included within an existing arms control regime. Our envisioned structural framework is what constitutes the novelty of our model and endows it with capacity to keep pace with modern weapons development.

We propose establishment of an independent, regulatory institution – an International Arms Control Agency for Software-Based Weaponry (IACA) – with robust competencies for treaty compliance verification and enforcement. The IACA would preside over a registration protocol requiring SBW possessors to register functional SBW software specifications for IACA certification of compliance with treaty regulations. Recertification would be required upon modification, ensuring continual compliance even as technology progresses. The IACA would have authority to mandate periodic and random inspections and would have sophisticated verification capabilities, such as satellite surveillance, at its disposal.

The IACA would also enforce compliance. It would have an adjudicatory body, investigating both Agency-identified violations and claims of violation made by treaty parties. This body would have the authority, subject to appeal, to issue binding decisions and proscribe remedies and sanctions, including enjoining deployment and international sale of SBW found to be in violation of treaty regulations.

It would also have the power to recommend individual political and military leaders, as well as private sector manufacturers, to relevant treaty-external bodies, such as the International Criminal Court, for investigation in such cases where SBW use transgresses treaty provisions in a manner violative of international criminal law. The treaty might also propose a novel strict liability provision for specific instances of grave violation, such as preemptive use of SBW to initiate a large-scale attack on civilian infrastructure, or gross negligence, such as permission of SBW capabilities to be hacked leading to large-scale disruption to civilian infrastructure.

In this way, the IACA would both verify and enforce enduring compliance, as well as facilitate trust-building transparency. To ensure objectivity, membership of the adjudicatory body would be regularly rotated and staffing of technical experts investigating possible violations would be comprised of individuals from a variety of nations, including the one under investigation. IACA decisions would also be subject to appeal considered by an appellate body.

V. Conclusion

SBW present a clear and present danger to world peace. Because the current arms control paradigm cannot effectively address the novel characteristics of SBW, a new paradigm is needed to accommodate the dynamic challenge of SBW evolution. An independent global regulatory entity should be established to implement a modernized arms control framework tailored to the contemporary and future realities of SBW. Such regulation should be a continuous process that is responsive to the evolution of SBW technology. In this paper, we have endeavored to introduce a preliminary sketch for such a model, which we hope will stimulate much-needed new discussion on this critical issue.

Endnotes

[1] Nathan Strout and Joe Gould, "Space Force Seeks $832 Million in Classified Spending, New Missions and More in Annual Wish List," *C4ISRNET*, June 4, 2021, Space Force seeks $832 million in classified spending, new missions and more in annual wish list (c4isrnet.com)

[2] James A. Acton, "Escalation Through Entanglement: How the Vulnerability of Command and Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security*, Vol. 43, Iss. 1 (2018), https://carnegieendowment.org/2018/08/08/escalation-through-entanglement-how-vulnerability-of-command-and-control-systems-raises-risks-of-inadvertent-nuclear-war-pub-77028

[3] Joe Schoneman, "Beyond Counterspace: Addressing Debris as a Credible Threat in Low Earth Orbit," *War on the Rocks*, November 16, 2020, https://warontherocks.com/2020/11/beyond-counterspace-addressing-debris-as-a-credible-threat-in-low-earth-orbit/

[4] Sydney J. Freedberg Jr., "Meet the Army's Future Family of Robot Tanks: RVC," *Breaking Defense*, Nov. 9, 2020, https://breakingdefense.com/2020/11/meet-the-armys-future-family-of-robot-tanks-rcv/

[5] Amit Katwala, "The U.S. Air Force is Turning Old F-16s Into Pilotless AI-Powered Fighters," *Wired*, June 27, 2020, https://www.wired.co.uk/article/f-16-us-air-force-qf-16

[6] Jon Harper, "Navy Has High Hopes for Robotic Ships," *National Defense*, Feb. 26, 2021, Navy Has High Hopes for Robotic Ships (nationaldefensemagazine.org)

[7] Farnam Street Blog, *The OODA Loop: How Fighter Pilots Make Fast and Accurate Decisions*, The OODA Loop: How Fighter Pilots Make Fast and Accurate Decisions (fs.blog)

[8] Shane Harris, "Black Market for Malware and Cyber Weapons is Thriving," *Foreign Policy*, March 25, 2014, Black Market for Malware and Cyber Weapons is Thriving – Foreign Policy

[9] Matan Mimran, "The Long-Term Threats Posed by the Vault 7 Leaks," *Cybereason*, Sept. 26, 2017, https://www.cybereason.com/blog/vault-7-leaks-long-term-threats

[10] United States Department of Defense, *Nuclear Posture Review* (February 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

[11] Maggie Miller, "Biden Budget Request Calls for Major Investments in Cybersecurity, Emerging Technologies," *The Hill*, April 9, 2021, https://thehill.com/policy/cybersecurity/547344-biden-budget-request-calls-for-major-investments-in-cybersecurity

[12] United States Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision For U.S. Cyber Command* (February 2018), https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

[13] Bilyana Lilly and Joe Cheravitch, "The Past, Present and Future of Russia's Cyber Strategy and Forces," EP-68319, *RAND* (2020), https://www.rand.org/pubs/external_publications/EP68319.html; Lyu Jinghua, "What Are China's Cyber Capabilities and Intentions," *Carnegie Endowment for International Peace* (2019), https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

[14] German Federal Foreign Office, *Capturing Technology: Rethinking Arms Control*, https://rethinkingarmscontrol.de/

[15] Geneva Internet Platform DigWatch, *GGE on Lethal Autonomous Weapons Systems*, https://dig.watch/process/gge-laws

[16] Geneva Internet Platform DigWatch, *GGE on Lethal Autonomous Weapons Systems*

[17] Human Rights Watch, *Killer Robots: Growing Support for a Ban*, August 10, 2020, https://www.hrw.org/news/2020/08/10/killer-robots-growing-support-ban

[18] Isabelle Khurshudyan, John Wagner, Colby Itkowitz, Eugene Scott, and Amy Wang, "Biden, Putin Hold 'Positive' Summit, But Divisions Remain Over Human Rights, Cyberattacks, Ukraine," *The Washington Post*, June 16, 2021, https://www.washingtonpost.com/politics/2021/06/16/biden-putin-live-updates/

[19] Vladimir Soldatkin and Steve Holland, "Far Apart at First Summit, Biden and Putin Agree to Steps on Cybersecurity, arms control," *Reuters*, June 16, 2021, https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/