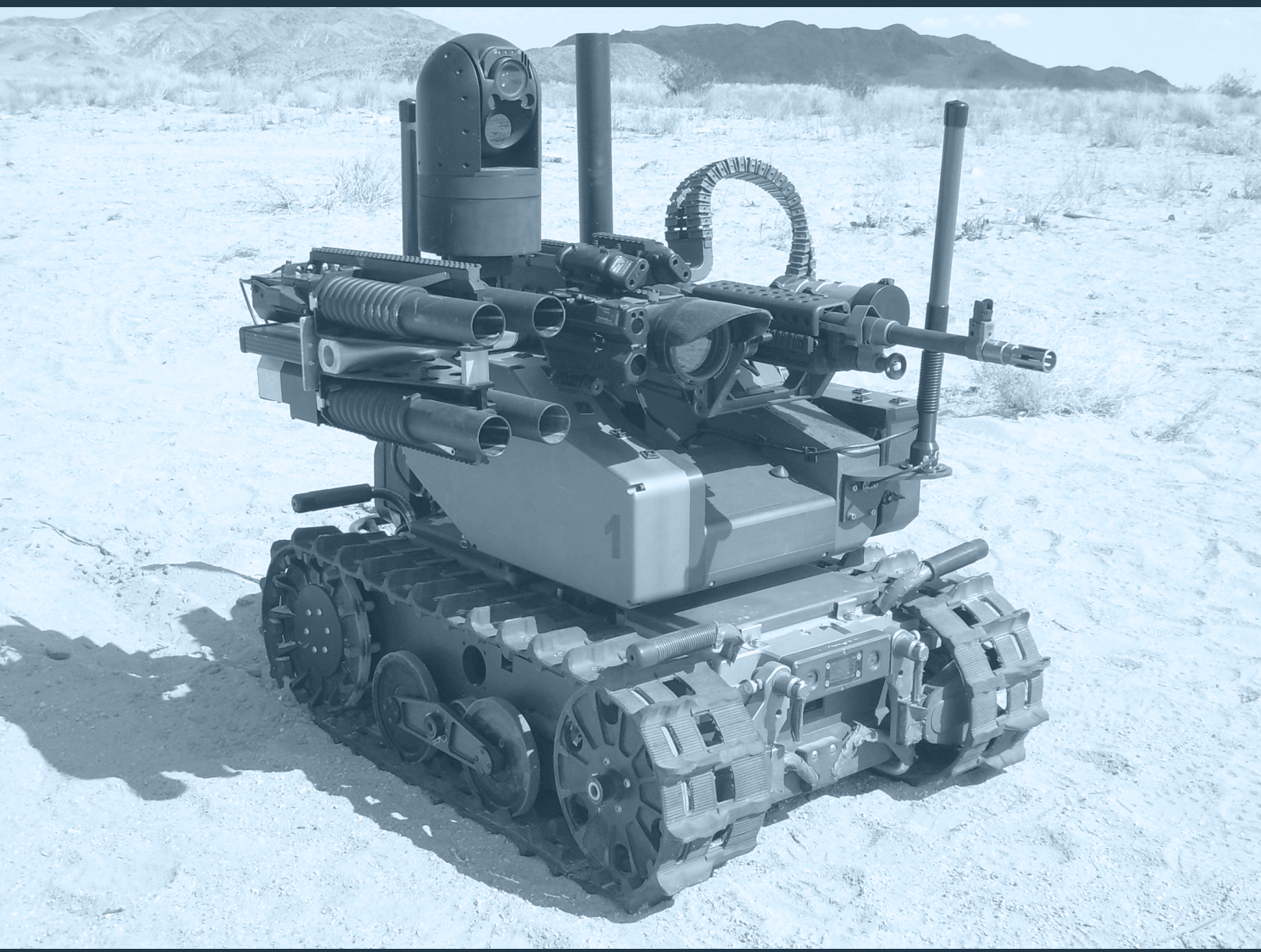
GCSP
Geneva Centre for Security Policy

OCTOBER 2018 | ISSUE 2

Strategic Security Analysis

Perils of Lethal Autonomous Weapons Systems Proliferation: Preventing Non-State Acquisition

Author: Philip Chertoff



www.gcsp.ch

Key Points

- Lethal Autonomous Weapons Systems (LAWS) promise significant military advantages to developing states.
- Many states have significant ethical and legal concerns about the potential for systems to destabilise conflicts and inflict collateral damage.
- Malicious non-state actors also have the potential to leverage LAWS for significant military advantage against state actors and acts of terror.
- The international community has not focused adequate attention on the potential for LAWS to proliferate to malicious non-state actors.
- The international community should implement export controls on LAWS, through the Wassenaar arrangement, to reduce the risk of transfer to malicious non-state actors.

Author Bio

Philip Chertoff is a J.D. candidate at Harvard Law School. During the spring of 2018, he was a Young Leader in Foreign and Security Policy at the Geneva Centre for Security Policy, where he researched autonomous weapons systems and emerging technology issues. Previously, he worked as an associate fellow with the GLOBSEC Policy Institute, where he initiated and managed the Cyber research program. Mr. Chertoff received his bachelor's degree in political science, with honours, from the University of Chicago.

The author thanks Dr Jean-Marc Rickli for his valuable comments and insight during the writing of this analysis, and the staff of the GCSP for their assistance during the fellowship.

1. Introduction

Terrorist groups, illicit organisations, and other non-state actors have a long fascination with advanced weapons technologies. In the early 90s, the Japanese death cult Aum Shinrikyo pursued multiple avenues to develop chemical, nuclear and biological weapons, eventually succeeding in the creation and deployment of Sarin gas.[1] Throughout the late 90s, Osama bin Laden and al-Qaeda allegedly made numerous attempts to acquire nuclear material from illicit actors. Starting in 2004, Hezbollah has been deploying Iranian-made, military-grade drones for surveillance and engagement.[2]

Despite the relative success of less sophisticated weapons, and the substantial expense and difficulty of acquisition for more advanced systems, non-state actors continue to pursue advanced weapons for two significant reasons. For less funded, less powerful non-state actors, advanced weapons substantially increase the scale of the force they can wield against enemies—they promise to "level the playing field". Advanced weapon systems also offer a significant reputational and symbolic benefit to non-state actors, as the ownership of such weapons confer a status limited to only a handful of powerful nations. States have long recognised these risks, and established numerous arms and export controls to restrict and regulate the transfer of massively destructive weapons.

However, international efforts to restrict proliferation of such weapons are currently lagging behind the emergence of new, possibly as-destructive, technologies. In particular, the last few years have marked the rapid development of lethal autonomous weapons systems (LAWS). Considering their potential to escalate conflicts and inflict massive collateral damage, the international community has long been debating necessary restrictions on the implementation of autonomy in weapons systems, even considering a ban on fully-autonomous systems. However, such conversations have largely been limited to state use. The international community has been painfully slow to address the possible acquisition and use of LAWS by non-state actors.

2. UN Efforts to Control Lethal Autonomous Weapons Systems

Between April 9th and 13th 2018, signatories to the UN Convention on Certain Weapons (CCWUN) and civil society organisation members met to participate in the 2nd Group of Government Experts (GGE) discussion of LAWS. The purpose of the GGE is to explore the technologies of LAWS within the context of the Convention (i.e. identify those relevant principles or restrictions applicable to lethal autonomous weapons systems). In all, outside of debate on an outright ban, discussions at the second GGE revolved around responsible state behaviour regarding LAWS. Conversation touched on responsible state development of systems, respect for international humanitarian law and requirements for human control at certain points of weapon operations. Despite these discussions on a number of points of state behaviour, participants did not adequately address another—state transfer. Specifically, the GGE did not adequately address the possible diversion of these systems and the risk of their proliferation to malicious, non-state actors.

3. Malicious Actors and LAWS

Academics, defence industry representatives and AI developers have all raised concerns about the possible acquisition of LAWS by malicious actors. In the 2015 expert meeting, GCSP's AI expert, Jean-Marc Rickli, warned about the value such systems offer to non-state actors and the risks of potential acquisition—including their possible use for indiscriminate violence and terrorist acts.[3] Before the first GGE, Elon Musk and other AI developers issued an open letter that specifically cited the significant risk that LAWS will become "weapons that despots and terrorists use against innocent populations".[4]

Yet, during the second GGE, acquisition by non-state actors, such as terrorists, was highlighted only in a few throwaway lines by certain representatives. This general absence was surprising, not just because of the significant attention to malicious actors in conversations prior to the second GGE, but also because of the significant risks posed by malicious use of LAWS. As Germany stated, in one of the few comments on malicious actors, LAWS could "exacerbate the threat of terrorism" and expand terrorist capacity to "indiscriminately inflict harm and inflict terror on civilians".[5]

The risk of disastrous use of LAWS by non-state actors is far greater than potential misuse by state actors. For professionalised militaries, like those of the US, UK, France, Russia, and China, command and subordination are requirements for the introduction of any new weapons systems. Any fully-autonomous weapons systems currently under development are likely a long way from integration into active engagement because professional state militaries need assurances of predictability and reliability. For malicious actors, however, concerns about predictability and reliability are less pressing, especially if LAWS could be a force multiplier in their asymmetric conflict. Malicious non-state actors have no need to account for proportionality or distinction in their attacks and, for terrorist groups, such indiscriminate violence may be the goal, as such brutality would cultivate the fear and intimidation that is integral to their missions.

4. LAWS and Proliferation

Some may believe that the acquisition of LAWS by malicious actors is a distant reality. However, such views fail to consider both the current proliferation of increasingly autonomous weapons systems, as well as concentrated efforts by malicious actors to acquire offset systems. The proliferation of LAWS should not be thought of as a watershed event; instead, it is a developing process of increasing autonomy in weapons systems. Currently, there are already weapons systems that operate with a degree of autonomy that might be considered characteristic of LAWS. Israel has developed two semi-autonomous drone systems, Harpy and Harop, which operate as "loitering munitions". These systems "loiter" around a target area, searching for targets, and engage when targets are located. Harpy and Harop have been used, or are currently in-use, by a number of countries such as China and Azerbaijan, and have been deployed in active conflicts.[6]

Autonomy is also winding its way into ground munitions and missile technology. South Korea has two such weapons in use. The SGR-A1 is a semi-autonomous sentry gun that offers automated targeting.[7] The Super aEgis II sentry turret was originally designed with fully autonomous capacity.[8] Since 2005, the British RAF has operated the Brimstone missile system, which offers an "indirect targeting" mode.[9] Increasingly, autonomous systems are being implemented in active conflicts. As development continues towards the creation of fully-autonomous systems, systems will offer ever-increasing autonomy in each iteration.

Active pursuit of offset systems by non-state actors has always been a significant concern. Theoretically, illicit actors need to pursue increasingly advanced technologies in order to stay ahead of their enemies. Bruce Hoffman observed, "success for terrorists is dependent on their ability to keep one step ahead of not only the authorities but also counterterrorist technology." Non-state actor pursuit of autonomous weapons is then not a question of if, but when. Hamas, Hezbollah and ISIS have already demonstrated the deployment of armed, remote-controlled drone systems.[10] The New York Times recently reported that the Islamic State has developed a homebrewed armed drone program, using modified off-the-shelf drone systems to drop bombs on, or kamikaze strike, Allied forces.[11]

It is highly unlikely that any state currently considering the development of LAWS can be persuaded to disengage from such activity based on the risk of malicious acquisition. Recognizing this, international efforts are largely focused on wrangling states to develop them with responsible use and ethical considerations in mind. For all the same concerns about ethics, international law, and strategic stability, it is as important that states take future proliferation to malicious non-state actors seriously. Nations should consider the creation of a harmonised export control regime for military-grade LAWS, and critical LAWS components, to reduce the risk of technology transfer to malicious actors.

5. Wassenaar: An International Export Control For LAWS?

By controlling exports, states can reduce the risk that developing LAWS will be diverted to prohibited actors.

States have long used export controls to regulate the transfer of sensitive goods, technology or services to other hostile actors (state and non-state). While export controls often target weapons with mass destruction capabilities or potential for destabilisation, some restrict the transfer of dual-use technology. Such controls originated in the Soviet era to prevent technology transfer to the USSR. In the post-Soviet era, these controls are often meant to block sensitive technology transfer to illicit actors, like terrorists. Considering the significant potential for LAWS to support illicit actors, there is a strong case for the implementation of multi-lateral export controls to restrict the transfer of military-grade LAWS and critical LAWS components to trusted state actors.

By controlling exports, states can reduce the risk that developing LAWS will be diverted to prohibited actors. Like most international agreements, the negotiation of a new export control regime would likely be a long and exhaustive process. Recognising this, the Wassenaar Arrangement, provides a ready platform for the near-term creation of a new export control on LAWS and critical LAWS components.

The Arrangement maintains a list of dual-use goods and technologies that all signatories agree to incorporate into their respective national export control lists. Dual-use items that fall under this list include certain types of explosives, sensors and circuits, and unmanned underwater vehicles. Commercial enterprises seeking to transfer listed items must obtain an export license and all transactions are closely monitored by national export authorities. States agree to "report on the transfers and denials of controlled items to parties outside the Wassenaar arrangement" and "exchange information on sensitive dual-use goods and technologies".[12] States are also guided by Wassenaar best practices, which include controls for ensuring that exported equipment is not diverted to unintended users.There is a valid criticism of the Wassenaar Arrangement, that export controls on LAWS could restrict civilian research on autonomy and artificial intelligence. This argument demonstrates the challenge at the heart of regulating dual-use technologies: they have both civilian and military applications. Regulation of dual-use technology requires detailed attention to language, in order to foster the benign, and restrict the malicious. The primary evidence for such criticism is the ill-fated 2013 amendment to Wassenaar, which, in the pursuit of stronger controls over the export of surveillance products, accidentally criminalised many of the necessary tools for stopping malware.

6. Lessons from the 2013 Amendment

The 2013 amendment issue hinged upon a failure to adequately characterise intrusive surveillance software. By including technology involved in the development of intrusion software, drafters allowed the interpretation that the amendment would apply to any code that made use of a software vulnerability. The resulting amendment significantly threatened legitimate security research and the ability to resolve software vulnerabilities. In December 2017, after protests from the security community, the U.S. government was finally able to convince other Wassenaar members to agree to a set of changes. The new language and exemptions satisfied a number of community concerns, but others still persist. The episode stands as a painful lesson on the consequences of regulatory overreach.

It would be unfair, however, to use the 2013 amendment as an argument against regulation of dual-use technologies (or, in this case, dual-use code). Rather it should be taken as a lesson on the need to carefully define additions to export control lists. The initial definition of "intrusion software" and the "technology involved in development" did not effectively meet three of the four criteria that confirm Wassenaar could control export of an item. "Technology involved in the development of intrusion software" was widespread outside Wassenaar participating states.[13] Availability would also prevent any effective control over transfer. By failing to make a "clear and objective specification of the item," the language of the control unintentionally folded in benign dual-use technologies. It was only after the 2017 amendment focused the item definition that the control on "intrusion software" more adequately met these criteria.

By contrast, military LAWS fall more neatly within the control criteria. LAWS are not currently identified or controlled by any other export control regime. There is limited research and development of military LAWS, like Super aEgis II or Brimstone, outside of Wassenaar members (or states with controls that are aligned to Wassenaar). This is in part due to the limited number of researchers with the necessary expertise and their increasing concentration within a few private and academic institutions.[14] The few states developing such systems would allow for effective control over exports. Finally, the definition of LAWS, with careful crafting, could be effectively defined such that states can clearly identify, monitor, and regulate transfers of the technology.[15]

Internal Innovation versus External Acquisition

Arguably the most significant criticism is that export controls would be ineffective for controlling the real vector for non-state acquisition: modification of commercial technology. All the necessary components to build an autonomous drone are available off-the-shelf or online. Cases of Mexican cartels and ISIS modifying commercial drones for combat use are well documented.[16] However, such a claim mischaracterises the technology adoption process. As Brian Jackson identifies in his study of terrorist innovation, technological acquisition is not a straightforward process (demonstrated by the difficulties of technological adoption in the civilian sector).[17] There are two primary mechanisms for technology uptake: internal innovation and external acquisition.

Internal innovation requires that the innovating entity have both the explicit knowledge of the technology (such as a blueprint or manual) as well as the tacit knowledge (experience or intuition from working with the technology).

Scholars and officials have expressed concern over online access to drone blueprints and machine learning algorithms, which non-state actors could use to build autonomous weapons.[18] However, to effectively innovate these technologies internally, non-state actors still require the tacit knowledge.

Underdeveloped tacit knowledge may explain why internal innovation by non-state actors has been largely unsophisticated. In the known cases of modified drones, the sophistication of the modification is quite low. The aforementioned cartel drone carried a bomb “via a string”, which was then detonated with a separate radio frequency detonator. ISIS drones do not demonstrate an advanced ability for modifying munitions delivery. Unsophisticated tools can be useful to non-state actors (and as mentioned unpredictable LAWS could support the actor’s mission), but they do not achieve the force capability and symbolic legitimacy that malicious non-state actors often desire when seeking advanced weapons systems. An illustrative case of the need for explicit and tacit knowledge is ISIS’s acquisition of chemical weapons. Starting in 2015, ISIS has been successfully delivering chemical warfare agents through a projectile delivery system.[19] However, this success was not the result of an innovative internal weapons program, but rather the end result of nearly two decades of research into these systems by Iraqi Sunni militant groups—a long process that required the both the internal development of explicit and tacit knowledge.

Computational weapons, in particular, have always proved challenging for non-state actors to develop internally. Experts have long been concerned about terrorist offensive cyber operations. ISIS hackers, however, have demonstrated a reliance on acquiring these capabilities from the Dark Web, because they have been largely incompetent at internally developing hacking tools or malware.[20] Such behaviour appears to indicate that ISIS and similar actors, while they may have access to the explicit knowledge to create LAWS, lack the tacit knowledge to effectively create and implement them in the near future. Yet, in the absence of being able to develop these weapons internally, these actors still retain the option and the ability to acquire them externally.

7. Conclusion

Nothing here is a perfect solution. Export controls are not flawless instruments for controlling the spread of dual-use technology, and the Wassenaar Arrangement is certainly not a flawless export control regime. But we should not make the perfect the enemy of the good. Controls and regulations to prevent the spread of certain weapons are like overlapping sieves: by constructing enough sieves, enough constraints on acquisition, states can raise the cost of entry to malicious non-state actors.

Recognising their potential for indiscriminate carnage, it is critical that states work to limit illicit transfer of near-autonomous or autonomous military systems. Implementing export controls on LAWS will require careful consideration and consultation, but successful controls can help reduce the near-term risk that malicious actors could wield this technology for violent ends—and allow for the peaceful development of tools for enriching our lives.

References

1 Danzig, et al. "Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons," July 2011. https://www.cnas.org/publications/reports/aum-shinrikyo-insights-into-how-terrorists-develop-biological-and-chemical-weapons

2 Plaw, Avery, and Elizabeth Santoro. "Hezbollah's Drone Program Sets Precedents for Non-State Actors." Jamestown, November 10, 2017. https://jamestown.org/program/hezbollahs-drone-program-sets-precedents-non-state-actors/.

3 Rickli, Jean-Marc. "Some Considerations of the Impact of LAWS on International Security: Strategic Stability, Non-State Actors and Future Prospects." presented at the Meeting of Experts on Lethal Autonomous Weapons Systems, Convention on Certain Conventional Weapons, United Nations Office Geneva, April 16, 2015. https://www.unog.ch/80256EDD006B8954/(httpAssets)/B6E6B974512402BEC1257E2E0036AAF1/$file/2015_LAWS_MX_Rickli_Corr.pdf.

4 "An Open Letter to the United Nations Convention on Certain Conventional Weapons." Future of Life Institute. Ac-cessed June 15, 2018. https://futureoflife.org/autonomous-weapons-open-letter-2017/.

5 Permanent Representation of the Federal Republic of Germany to the Conference on Disarmament in Geneva. "Statement Delivered by Germany on Security Dimension and Options." presented at the 2018 Group of Governmental Experts on LAWS, Convention on Certain Conventional Weapons, United Nations Office Geneva, April 13, 2018. http://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/statements/13April_Germany.pdf.

6 Gibbons-Neff, Thomas. "Israeli-Made Kamikaze Drone Spotted in Nagorno-Karabakh Conflict." Washington Post, April 5, 2016, sec. Checkpoint. https://www.washingtonpost.com/news/checkpoint/wp/2016/04/05/israeli-made-kamikaze-drone-spotted-in-nagorno-karabakh-conflict/; China, having purchased the Harpy system in the 90's, developed its own loitering weapons system, the ASN-301. Dombe, Ami. "China Unveils a Harpy-Type Loitering Munition." Israel Defense, January 3, 2017. http://www.israeldefense.co.il/en/node/28716.

7 Some claim that the SGR-A1 actually offers an autonomous engagement mode, a claim that creator Samsung Techwin vehemently denies. Velez-Green, Alexander. "The Foreign Policy Essay: The South Korean Sentry—A 'Killer Robot' to Prevent War." Lawfare, March 1, 2015. https://www.lawfareblog.com/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot-prevent-war.

8 It was later updated with safeguards requiring human target approval, based on customer requests. Parkin, Simon. "Killer Robots: The Soldiers That Never Sleep." Accessed June 15, 2018. http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep.

9 "Brimstone." Missile Threat. Accessed June 15, 2018. https://missilethreat.csis.org/missile/brimstone/.

10 Altmann, Jürgen, and Frank Sauer. "Autonomous Weapon Systems and Strategic Stability." Survival 59, no. 5 (September 3, 2017): 127. https://doi.org/10.1080/00396338.2017.1375263.

11 Schmitt, Eric. "Papers Offer a Peek at ISIS' Drones, Lethal and Largely Off-the-Shelf." The New York Times, December 22, 2017, sec. World. https://www.nytimes.com/2017/01/31/world/middleeast/isis-drone-documents.html.

12 "About Us." The Wassenaar Arrangement. Accessed June 15, 2018. https://www.wassenaar.org/about-us/.

13 Criteria for the Selection of Dual-Use Items (2004). https://www.wassenaar.org/app/uploads/2015/06/Criteria_for_selection_du_sl_vsl.pdf.

14 Vincent, James. "Tencent Says There Are Only 300,000 AI Engineers Worldwide, but Millions Are Needed." The Verge, December 5, 2017. https://www.theverge.com/2017/12/5/16737224/global-ai-talent-shortfall-tencent-report.

15 Current efforts to define LAWS have stalled within the UN GGE, largely driven by concerns from some states that an overly broad definition would restrict present development and implementation plans. Within an export control, such a definition could be made more inclusive in the interest of carefully monitoring both lethal autonomous and lethal near-autonomous weapons systems. One caveat would be that such a definition would be exclusive of digital LAWS (the possible creation of non-deterministic, worm-like cyber threats that lethally and non-lethally engage targets). In much the same way that the 2013 amendment was not an effective method for restricting the spread of intrusion tools, a new amendment that would attempt to restrict digital LAWS would likely fail (anyone who has been attacked can copy and share the relevant code). This differs from the code for physical LAWS, which would require the sharing of relevant code by the creators (or acquisition and reverse-engineering of a system) in order to be copied and spread.

16 Mizokami, Kyle. "Mexican Drug Cartels Are Turning Drones Into Flying Bombers." Popular Mechanics, November 1, 2017. https://www.popularmechanics.com/military/weapons/a28874/drug-cartels-drones-into-bombers/; Schmitt, Eric. "Pentagon Tests Lasers and Nets to Combat a Vexing Foe: ISIS Drones." The New York Times, December 22, 2017, sec. World. https://www.nytimes.com/2017/09/23/world/middleeast/isis-drones-pentagon-experiments.html.

17 Jackson, Brian A. "Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption." Studies in Conflict & Terrorism 24, no. 3 (May 1, 2001): 183–213. https://doi.org/10.1080/10576100151130270.

18 Weaver, Nicholas. "'Slaughterbots' and Other (Anticipated) Autonomous Weapons Problems." Lawfare, November 28, 2017. https://www.lawfareblog.com/slaughterbots-and-other-anticipated-autonomous-weapons-problems; Michael C., Horowitz. "Who'll Want Artificially Intelligent Weapons? ISIS, Democracies, or Autocracies?" Bulletin of the Atomic Scientists, July 29, 2016. https://thebulletin.org/who%E2%80%99ll-want-artificially-intelligent-weapons-isis-democracies-or-autocracies9692.

19 Strack, Columb. "The Evolution of the Islamic State's Chemical Weapons Efforts." Combating Terrorism Center at West Point, October 18, 2017. https://ctc.usma.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/.

20 "ISIS Hackers Handicapped by Poor Coding Skills and Hopeless Encryption Tools." TEISS, September 27, 2017. https://teiss.co.uk/news/isis-hackers-poor-coding-skills/.

GCSP
Geneva Centre for Security Policy

Where knowledge meets experience

The GCSP Strategic Security Analysis series are short papers that address a current security issue. They provide background information about the theme, identify the main issues and challenges, and propose policy recommendations.

Geneva Centre for Security Policy - GCSP
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
CH-1211 Geneva 1
Tel: + 41 22 730 96 00
Fax: + 41 22 730 96 49
e-mail: info@gcsp.ch
www.gcsp.ch