LAWS and Export Control Regimes: Fit for Purpose?

iPRAW Working Paper – April 2020

The International Panel on the Regulation of Autonomous Weapons (iPRAW) is an independent, interdisciplinary group of scientists working on the issue of lethal autonomous weapon systems (LAWS). It generally aims at supporting the current debate within the UN Convention on Certain Conventional Weapons (CCW) with scientifically grounded information and recommendations – looking at a potential regulation of LAWS from different angles.

Broadening the scope of regulatory options (here: outside of the CCW), this working paper links iPRAW's existing recommendations on human control in the use force to deliberations on export controls for LAWS (i.e. weapon systems with 'autonomy' in their targeting functions) and technological components relevant to LAWS. We highlight some effects of the diffusion[1] or transfer of LAWS and the potential role of national and multilateral export control regulations as a means of mitigating the challenges related to the development and use of LAWS.[2] We also explore the special challenges to the effective implementation of export controls on software based, data-driven technologies, in particular with regard to the general-purpose use of many of the enabling components. With that in mind, we identify and discuss how export control regimes could provide guidance to the participating states on the issue of LAWS.

This paper is focused on the specific enablers of autonomous functions, which could be, for example, hardware components like sensors and processors, software, training data, and/or technical expertise. Those functions can be applied to various weapon platforms that, in some cases, might already be covered by existing export controls due to their range, velocity, mobility, payload or other variables. The focus on functions adds a layer to this or broadens the scope of exports controls.

Reasons for Export Controls on LAWS

Generally, iPRAW is concerned with *arms control* regulations for LAWS, especially in the context of the CCW. We call for the implementation of human control in the use of force to enable the application of international humanitarian law (IHL), as well as for operational and ethical reasons. iPRAW has suggested minimum requirements for human control, notably "control by design" and "control in use".[3] Control by design restricts technical and military capabilities through deliberate design choices, in particular autonomous functions in the target selection and engagement process. Control in use implies the implementation of human control

---

1 We use the term *diffusion* instead of *proliferation*, since the term *proliferation* is mostly used with regard to nuclear weapons or weapons of mass destruction and we would like to avoid the assumptions and concepts related to this term. In the context of this brief working paper, we chose to focus on exports, excluding other types of transfer like diversions or theft.

2 For a broader overview of current challenges to export control regimes see e.g. Kolja Brockmann (December 2019), *Challenges to Multilateral Export Controls. The Case for Inter-regime Dialogue and Coordination*, SIPRI, available online at <https://www.sipri.org/sites/default/files/2019-12/1912_regime_dialogue_brockmann.pdf> (April 23rd, 2020).

3 See e.g. iPRAW (August 2019), *Focus on Human Control*, available online at <https://www.ipraw.org/wp-content/uploads/2019/08/2019-08-09_iPRAW_HumanControl.pdf> (April 23rd, 2020).

through procedures during attack – both steps require situational understanding and options for human intervention during operation.

While a humanitarian arms control regulation based on this principle would address the development and use of LAWS, export controls would focus on the international distribution of the weapon system, its components or know-how on developing such systems. Both, however, might follow the same **objective to foster the application of human control in the use of force**.

With or without a regulatory framework for the use of LAWS, producers of these weapon systems might not be able to restrict the IHL-conform usage of their products through deliberate design choices (and limitations) only. **At the point of sale, a producer/seller/trader of a weapon system with autonomous functions (in the selection and engagement of targets) cannot guarantee the level of control humans will exercise during the use of those weapons**. Therefore, the diffusion of LAWS could trigger an erosion of a potential qualitative arms control regulation (e.g. a CCW protocol), especially if such a regulation only relies on national implementation and national verification. This is a blind spot in CCW deliberations and possible future regulations within this framework. Consequently, it needs to be addressed separately. Thus, the goal of export restrictions and export control could be to uphold the principle of human control over the use of force by hampering the diffusion of autonomous (targeting) functions in weapon systems. Criteria like the risk for violations of IHL or human rights apply to arms transfers already, but in the case of LAWS the lack of clarity over the adequate level or type of human control necessary to ensure compliance with IHL (as illustrated by the CCW debates) would complicate export controls further.
Even if no prohibition of the development and use of LAWS exists, at least the transfer of the enabling technologies could be restricted to mitigate the challenges of LAWS to IHL.

A number of open questions present themselves with regard to export controls for LAWS:

- Could or should provisions in **existing** national or multilateral export control regulations be expanded to the specifics of LAWS and technologies enabling autonomous functions in weapon systems?
- Could or should there be a **new multilateral instrument** to restrict the transfer of this type of weapon or enabling technologies?
- What weapon systems or technologies could or should be **subject** to such an instrument to limit diffusion? Can LAWS be broken down into single components in a regulation?

Elements of Export Regulations

We analyze four multilateral export control regimes: the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (WA) on conventional arms and dual-use goods, the *Missile Technology Control Regime* (MTCR) on delivery systems for weapons of mass destruction, the rules of the *Australia Group* on components for the production of chemical and biological weapons, and the *Nuclear Suppliers Group* on elements of nuclear weapons. They are based on lists of restricted technologies and thereby provide international provisions that member states translate into national export legislation.

The subject of an export regulation for LAWS could be the transfer of either a complete weapon system or components needed to assemble a weapon system with autonomous targeting functions. The components would include elements that can transform a civilian or general-purpose system (e.g. a car or a drone) into a weapon with autonomous targeting functions, such as hardware (platforms, sensors, actuators, processors), software (software programs and

algorithms, such as computer vision libraries), and technology like know-how (technical expertise, manuals for technology, technical assistance) and data (e.g. for training and testing machine learning algorithms, technical information).

Hardware relates to physical platforms and delivery systems, like aircraft, vehicles as well as sensors and processors and their components, but can also include production and testing equipment and materials.

Software refers to programs and algorithms of a (weapon) system. Software is a component of a weapon system that orchestrates the functions of the physical system. Its capabilities cannot be judged by using visible physical features and therefore could be easily altered. In other words, software can transform and enhance qualitative and quantitative functions of a weapon system without changing its physical dimensions.

Know-how comprises the knowledge and technical expertise on how to build and/or use a certain weapon system. This includes maintenance, training, and the actual operation of the machine as well as the training of personnel pertaining to research and development. At a more technical level, know-how entails the management of a system's complexity which refers to the system integration and the assembling of major technology enablers and their respective components.

Data is the basis for information about the world that system engineers can use to train data-driven systems with computational methods (e.g. artificial intelligence, machine learning). It also includes the information a system collects and uses to interact with the world while in operation. Beyond these categories a combination of them may constitute functions of a weapon system, particularly autonomous functions. Functions, in this case selection and engagement of targets without human control, could be declared as criteria for any restriction with regard to export control – yet they are difficult to define (and verify).

Options and Gaps of Export Control Tools

Export control regimes strictly define their subjects via technical characteristics such as physical parameters (e.g. weight, size, velocity, range, payload) and technical-military capabilities. The multilateral export control regimes have provisions on hardware, software, and technology which covers know-how and data. Most promising for the subject of LAWS are the provisions of the Australia Group for its catch-all clause and, especially, the Wassenaar Arrangement for its List of Dual-Use Goods and Technologies.

Even though the existing agreements and regimes do not offer full-fledged concepts regarding autonomous functions, they include some starting-points for LAWS nevertheless: **Hardware** is covered by all regimes, e.g. in the form of delivery systems and other specific equipment and components. Components that enable specific military capabilities are often of **dual-use** in nature and therefore enlisted in the control lists. Autonomous functions rely on specific components (sensors, processors, actuators), but those are enabling components for a variety of armament functions and not specifically for automation/autonomy.

Software is mentioned in every regime under consideration. Still, software as an enabler of autonomous functions has not been addressed by any export control provision so far. The WA could provide a starting point to capture those: It focuses on the applications of software in C³I and C⁴I that might offer some parameters delineating the military applications of AI software that should be covered such as "software specifically designed for military use and specifically designed for modelling, simulating or evaluating military weapon systems; […] simulating military operational scenarios; […] for Command, Communications, Control and Intelligence

(C³I) or Command, Communications, Control, Computer and Intelligence (C⁴I) applications."[4] Furthermore, in many cases the WA covers software that is required for the use of a listed weapon system. This can stir some issues with regard to the dual-use capacity of the software, depending on how specific it is to the military use.

Know-how is not specifically addressed in the multilateral export control regimes. It has only been referenced when it comes to building and/or assembling certain machines. The transfer of knowledge specifically applicable to the design and usage of systems with autonomous functions has not been addressed so far.

The export control regimes under consideration do not specifically mention machine-readable, labelled **data** for machine-learning algorithms. Yet, the export of data is regulated when it comes to enhancing performance of a specific system in the WA. The overall understanding of data in the considered regimes refers to technical information about the technology itself, but also information about the background and context of the technology used. The broader concept of data comprises the design and development of both individual components and the entire system.

Although export control of military capabilities at state level exists already, it leaves significant gaps in incorporating the possibly diverse types of LAWS design and development. One of the on-going points of exploration for the export control community since the 1970's has been the question of how to handle **intangibles**. While software for military use has been mostly proprietary in the past, major parts of software frameworks for e.g. machine learning are open source developments nowadays. That is why software or software components enabling autonomous functions, e.g. in target identification, classification or selection, can and are meant to proliferate globally for reasons of further development and application. Open source software and collaborative means of software development today can therefore impose significant challenges to the non-diffusion of military functionalities. While we need to better understand the cross-border nature of software diffusion and distribution by continuing to explore this question about intangibles, we also need to acknowledge the reality that critical technology of LAWS, which is likely heavily software-dependent, requires new and creative solutions perhaps unexplored by export control communities in the past.

Alongside or instead of hard law, soft-law norm setting instruments may be the most immediately scalable and practical approach. Two of such approaches to include a wide range of stakeholders and dissuade proliferation of LAWS are multi-stakeholder negotiations and open source licensing models. A **multi-stakeholder approach**[5] is of crucial importance since multiple sectors – the scientific, the commercial and the military – are involved in research and development of both the systems themselves as well as the components that make up a LAWS. In adapting existing export control regulation to the specifics of LAWS, all views need to be taken into account and issues of ethical, legal, security-related and technological nature have to be addressed.[6] This includes the actors potentially fielding these systems, the political decision-

---

4 Wassenaar Arrangement - Vol. II: *List of Dual-Use Goods and Technologies and Munitions List*, available online at <https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf> (April 23rd, 2020), p. 212, para. ML21 b.

5 **Caveat**: The export control community linked to the Biological Weapons Convention (BWC) presented a multi-stakeholder approach but were met by strong opposition within the biologist communities. We can learn lessons from their experience in terms of what made their multi-stakeholder initiative unpalatable to the particular community. While it is important to take the analogies from the BWC example, we are under the impression that there are strong signals indicating the interest in such multi-stakeholder engagement and initiative on the issues of LAWS.

6 Also see Brockmann (2019), p. 24 on track 1.5 discussions and inter-regime dialogues.

makers, and the military which procures, stations and operates it, should be part of that multi-stakeholder approach to ensure a comprehensive concept to the challenge at hand.

In addition to export controls, the adjustment of existing **open-source licensing models** could set basic conditions for the use and further development of software in the critical functions of the targeting process. Specific provisions for software and programming frameworks for e.g. object recognition and classification, face and subject identification in general, and change detection (to name a few), when published under a specific licensing model, could create awareness for responsible use amongst their users. Such licensing models could set obligations for end-users to transparently document the usage of the respective software or software component and ask for the implementation of sufficient human oversight in use. This blueprint or framework of code could provide the foundation for the development and distribution of enabling software components while still safeguarding the agreed baselines from the multi-stakeholder negotiations. For the implementation of such an open-source licensing model a multi-stakeholder commission or oversight board could be established to secure the proper usage and documentation of the source codes and could provide manufacturers with the required licenses and knowledge (if needed). Such a commission could be advised by a group of experts to keep track of changes and modify the open-source licenses in accordance with up-to-date research and developments. Regarding the current structure of the open source community, especially when comes to licenses for 'ethical' software, such an initiative appears to be quite challenging, though.[7]

CONCLUSION

In conclusion, we identify three main findings with regard to the role of export control in countering the diffusion of LAWS:

1. The need for new or adapted export control mechanisms and other provisions to stop the transfer or re-purposing of technologies enabling LAWS depends on the existence and efficiency of multilateral regulations, obligations to maintain human control over the use of force, and prohibitions with regard to the development, procurement and use of LAWS. Export control and other measures can only complement rather than replace (humanitarian) arms control regulations.
2. Current export control regimes do not cover LAWS sufficiently, although some aspects might be helpful in offering starting points. A complementary approach to list-based export controls is required due to the unique characteristics of LAWS and their essential technological components.
3. The framework that the multilateral export control regimes offer might be expanded to increase the coverage of enabling technologies required for LAWS and more explicitly include obligations relating to human control etc. in the criteria for licencing decisions and risk assessments.

iPRAW thanks Kolja Brockmann for his valuable remarks on a draft version of this paper.

The International Panel on the Regulation of Autonomous Weapons (iPRAW) is coordinated by:
Stiftung Wissenschaft und Politik (SWP) – German Institute for International and Security Affairs
Ludwigkirchplatz 3-4, 10719 Berlin, Germany
This project is financially supported by the German Federal Foreign Office.
Find all reports and more information online at **www.ipraw.org**.

[7] iPRAW thanks Cheng Lin for sharing her thoughts on that issue in a yet unpublished paper with us.