Focus on National Regulations on LAWS and Military AI

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Focus on National Regulations on LAWS and Military AI

August 2021

ABOUT IPRAW

Setting and Objectives: The International Panel on the Regulation of Autonomous Weapons (iPRAW) was founded in March 2017 and will run until June 2022. iPRAW is an independent group of experts from different nation states and scientific backgrounds.

The mission of iPRAW is to provide an independent source of information and consultation to the Group of Governmental Experts (GGE) within the framework of the United Nations CCW (*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*) during the ongoing process toward a possible future regulation of LAWS (lethal autonomous weapon systems). This work includes, but is not limited to, the provision of expertise on the military, technical, legal, and ethical basis for practical and achievable policy initiatives regarding LAWS. The mandate of the CCW's open-ended GGE on LAWS will guide the work of iPRAW.

iPRAW seeks to prepare, support, and foster a frank and productive exchange among participants, culminating in perspectives on working definitions and recommendations on a potential regulation of LAWS for the CCW GGE. iPRAW is independent from the GGE and does not function in any official capacity regarding the CCW.

Funding, Organization, and Participants: iPRAW is financially supported by the German Federal Foreign Office. The views and findings of iPRAW do not reflect the official positions of the German government or any other government. *Stiftung Wissenschaft und Politik – The German Institute for International and Security Affairs* (SWP) is organizing the panel. The participants have been selected on the basis of their expertise and the perspectives they bring from a wide range of professional and regional contexts. iPRAW represents a broad variety of views on the topic of autonomy in weapon systems. Its members have backgrounds in natural science, engineering, law, ethics, political science, and military operational analysis.

Scope: The panel acknowledges that LAWS may pose a number of considerable legal, ethical and operational challenges and that they might change the security environment in a fundamental way. The full potential of these weapon systems is yet unknown and a mutually agreed definition on LAWS does not exist.

In order to support the CCW GGE process, iPRAW works on approaches towards a potential regulation of LAWS. In this context approaches to regulations are construed broadly and can include both the application of existing international law as well as new legal instruments. This includes various issues, like requirements for human control over the use of force.

Procedure: The participants commit themselves to actively engage in and contribute to the meetings and the scientific dialogue related to iPRAW's activities. Papers with agreed upon recommendations on relevant issues will be published via the project's website (www.ipraw.org).

Communication and Publication: The participants discuss under the Chatham House Rule: participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed. As a matter of confidentiality, photographs, video or audio recordings are not allowed during iPRAW meetings.

The results of the panel discussions will be published. iPRAW members will strive to reach consensus on their recommendations and to reflect that in the panel's publications. Media inquiries with regard to official iPRAW positions should be directed to the steering group. Apart from that, the panel members are free to talk about their personal views on participation and the topics of the panel.

Learn more about iPRAW and its research topics on www.ipraw.org. Please direct your questions and remarks about the project to mail@ipraw.org.

CONTENT

EXECUTIVE SUMMARY

From a ban to a soft-law mechanism, any potential international regulation of LAWS could not be implemented without the support of national regulatory frameworks. Also, the creation of a multilateral regulation could benefit from understanding national challenges and solutions. To facilitate the discussion of implementable governance options for the UN Convention on Certain Conventional Weapons (CCW) debate on LAWS, this report provides an analysis of national regulations on LAWS and its enabling technologies. Rather than providing an exhaustive account of all relevant policies of States Parties to the CCW, the report focuses on the regulatory approaches of five States Parties (China, Japan, Russia, the United States, and Germany in conjunction with the European Union), highlighting common challenges as well as possible solutions. National regulations, reviewed by this report, include general strategies on (military) AI, rules on development and procurement, e.g. weapon reviews, rules on the deployment of LAWS and military AI, and export control. Moreover, the report also considers whether and how states shape and formulate regulations on human control and similar concepts in the use force. As states are only beginning to grapple with governing emerging technologies in the area of LAWS, such an overview may not only stimulate the GGE debate but also prove insightful for other states and lay the groundwork for exchanges on best practices and lessons learned.

Key Takeaways and Recommendations:

- ➢ Overall, **only few regulations directly address LAWS**. Instead, most policies cover aspects of enabling technologies of LAWS without directly considering weapon systems with autonomous functions.
- ➢ Several states have so far **focused on regulating non-military applications of AI** and have only briefly considered the militarization of AI and the issue of LAWS. Hence, the development of dedicated strategies and policies that consider military applications of AI and weapon systems with autonomous functions deserves further attention.
- ➢ A **multi-stakeholder approach** involving experts from civil society, including academia, and industry, can prove valuable in embracing and aligning different perspectives and formulating policies that are in line with law and ethics, practical and effective. As some states and organizations have relied

on such approaches already, it might be valuable to exchange best practices on these efforts.

➤ The extent to which states have put in place substantive **weapon review mechanisms** differs greatly, allowing for distinct approaches to – and perhaps even deficiencies in – system safety and robustness. Cross pollination of ideas and the sharing of best practices exercised across states on testing, evaluation and validation processes would be valuable. This should also entail knowledge exchanges on the special requirements for testing enabling technologies of LAWS.

➤ In light of the unique character of AI-based data-driven techniques and other technologies enabling machine autonomy, states should also scrutinize whether their **review criteria and verification, validation, test, and evaluation (VVT&E) practices** are fit for purpose when reviewing AI-infused systems and systems with autonomous functions, including the software and training data they rely on. Testing the reliability and predictability of such systems will require fundamentally different practices and criteria than those used for traditional weapon systems.

➤ At this stage, most regulations govern the **deployment** of LAWS only implicitly which may lead to distinct views on the use of LAWS and diverging deployment practices. Therefore, it would be beneficial for states to work towards a similar understanding around the question of how to deploy weapon systems with autonomous functions, exchange best practices on rules of engagement and the training of operators and commanders.

➤ Fundamental questions remain as to whether and how **export controls** can be designed and enforced to effectively curtail the proliferation of weapon systems with autonomous functions and their dual-use components. Clearly, the hardware-based methodology of traditional export control regimes is insufficient for addressing the proliferation of technologies that enable machine autonomy for military purposes. Therefore, independent studies and dedicated international multi-stakeholder discussions could enhance the understanding of how export control can be rethought to address the unique nature of software and other enabling technologies of LAWS.

Several of these steps require individual states to review and update their policies at the national level. However, especially when it comes to sharing best practices and experiences regarding the regulation of technologies in the area of LAWS, the GGE on LAWS would prove as an adequate forum for such international debates. For specific issues, discussions in other international fora could prove valuable as well, such as in the framework of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

1. INTRODUCTION

The debate of the Group of Governmental Experts (GGE) on lethal autonomous weapon systems (LAWS) within the UN Convention on Certain Conventional Weapons (CCW) has hitherto focused primarily on an international approach to regulating military AI and machine autonomy. Measures undertaken at the domestic level, such as legislative acts dealing with and addressing LAWS have not been discussed in the GGE in greater detail thus far. Within the GGE States Parties are invited to share national policies and practices that could prove insightful for the debate; and indeed on some occasions, weapon reviews undertaken at the domestic level have become part of the GGE debate.

Currently, hardly any national legislation or strategies specifically focused on LAWS exist. Therefore, this report analyzes policy measures on emerging technologies in the area of LAWS more broadly, conceptualizing military AI and machine autonomy as crucial enablers of LAWS (even though they are by far not the only ones). Accordingly, we only use the term LAWS when we specifically refer to those and not military AI and machine autonomy in general.

In seeking to further deepen this effort and to contribute to the debate on LAWS, this report sheds light on national approaches to regulating military AI and autonomy in weapon systems, highlighting common challenges as well as potential solutions. As part of this analysis, the report also considers whether and how states shape and formulate regulations on human control and related concepts in the use of force.[1]

Rather than providing a comprehensive analysis of all CCW States Parties, the report offers first steps towards reviewing the current state of national legislation on LAWS. It focusses on the national approaches of the following five CCW States Parties as case studies: the United States (US), Russia, China, Japan, and Germany in combination with the European Union (EU). Research on the specific case studies has been provided by iPRAW members Vadim Kozyulin (Russia), Heigo Sato (Japan), Binxin Zhang (China) and Lydia Wachs (Germany, EU, US), who drew on publicly available information in the respective countries' languages, including legal and policy documents, official statements, press releases, news reports and further secondary

---

[1]   For iPRAW's concept of human control and how it could be integrated in an international regulation see iPRAW (2021).

literature. The report relies exclusively on unclassified sources. Furthermore, by focusing on regulations and policies, the report does not aim to analyze the level of AI development in the respective countries.

Overall, the analysis demonstrates that a number of measures are already in place, but that certain loopholes remain, deserving greater attention. Several of these steps would require individual states to review and update their policies. Discussions in and regulation of multilateral fora will be crucial to develop a common understanding of the challenges and potential solutions.

While focusing on lethal autonomous weapon systems, iPRAW does not exclude a regulation of non-lethal force. By LAWS we refer to weapon systems with autonomy in their critical functions, meaning weapon systems without sufficient human control over the selection and engagement of targets.

To set the scene, section 2 examines key actors in the development of national positions and policies on technologies related to LAWS as well as challenges they identify in relation to LAWS. Section 3 analyses how the reviewed states approach technologies potentially applied in weapon systems with autonomous functions, focusing on specific regulations that are already in place and address the development, procurement, deployment and export thereof. Finally, section 4 presents iPRAW's conclusions and recommendations on how national measures can be strengthened to help develop international regulations on technologies related to LAWS.

2. ACTORS AND CHALLENGES

2.1. ACTORS

At the CCW GGE on LAWS, **national delegations** play a pivotal role in representing national approaches and positions on LAWS. These delegations are primarily composed of representatives from the respective Ministries of Foreign Affairs and the Ministries of Defense, sometimes drawing support from adjunct national experts.

These ministries – also outside the GGE – have played major roles in the debate on military AI and machine autonomy, for example by drafting strategy documents, hosting conferences, funding research projects or setting up new bodies. However, they are not the only actors informing national approaches on military AI and autonomy. Depending on the specific country, representatives from **other branches of the government**, parliament as well as civil society, including academia, and industry play important roles as well. Robotics and AI – likely key ingredients of LAWS development – are seen as enablers of industry 4.0 and the economic prosperity it promises. As such, it is not surprising to find that in several of the reviewed countries, those branches of government that focus on economic and social questions have been driving forces in the development of policy on AI. In Japan and Germany, in particular, the respective Ministries of Economic Affairs have played key roles in drafting the national AI strategies. As a consequence, these strategies only briefly touch upon AI for military purposes. This goes along with a relatively stronger focus on AI for commercial and social purposes of the respective governments and a less pronounced role of military AI. In Russia and the US, the analyzed sources show a stronger focus on military AI, indicating that military applications of AI have gained more attention in these countries.[2]

The countries under scrutiny of this report have also witnessed the creation of **new departments, bodies or ad-hoc committees** by the government, parliament or

---

[2]   See chapter 2. For another discussion of several European AI strategies, see e.g. Franke (2019).

individual ministries in order to encourage AI development and policy. This trend has been particularly pronounced in the US with the creation of new bodies focused on AI for military purposes, most importantly the Joint Artificial Intelligence Center (JAIC) coordinating the AI policy of the Department of Defense as well as the National Security Commission on AI (NSCAI) that was established as an independent body to review the role of AI for US national security. Similarly, in April 2021, the Russian Ministry of Defense announced plans to create a department focused specifically on AI development.[3] Also the Japanese Ministry of Defense established a division in 2020 that is tasked with developing and coordinating AI policy.[4] In Germany, the parliament has played a relatively stronger role i.e. by commissioning a report from the Office of Technology Assessment at the German Bundestag (TAB) – advising the German Parliament and its committees on questions relating to scientific and technological change – on the state of play in the development of LAWS as well as ethical and legal questions raised in this context.[5]

Beyond state actors, the **private sector** has informed national approaches to military AI and machine autonomy, albeit to different degrees and by assuming distinct roles. In some countries, private stakeholders have taken a clear stance on AI and its use for military purposes. In the **US**, for example, after a widely publicized protest by its employees, Google declared in 2018 that the company would not build AI for "weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people."[6] At the same time, Google's peers Microsoft and Amazon have appeared more willing to provide the military agencies with AI solutions.[7]

In **China**, Jack Ma, the founder of Alibaba, stressed repeatedly that technological innovation might drive global conflicts, and urged governments to "move fast" to tackle the risks posed by technological innovation.[8] Some Chinese researchers in the private sector, notably from Tencent and Baidu, have signed the "Future of Life" pledge.[9] There are furthermore a dozen of non-governmental initiatives on AI principles and ethical norms from academia and industry, including big tech companies, like Tencent and Baidu.[10]

In **Germany**, in the context of the European defense project FCAS, Airbus Defence and Space and the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) launched the FCAS Expert Commission on the responsible use of technologies in 2020. It has the objective to "determine ethical guidelines based

---

[3]   See RIA Novosti (2021).

[4]   See Japan Ministry of Defence (2020).

[5]   See Grünwald and Kehl (2020).

[6]   Brewster (2020).

[7]   See Anger (2018).

[8]   See Browne (2019); The Indian Express (2017).

[9]   See Future of Life Institute (2021).

[10] See e.g. BAAI (2019); Shanghai Municipal Science and Technology Commission (2019); Tencent Research Institute (2021); China IT News (2018).

on international law and to ensure their technical implementation"[11] in the project. The commission brings together stakeholders from ministries, the military as well as experts with technical, political, social science and legal backgrounds.

In **Russia**, the private sector has played a minor role and most efforts have been state-controlled or state-backed. For example, the state-controlled bank Sberbank has assumed a leading role in developing AI policy and encouraging AI R&D.[12]

2.2. CHALLENGES

While the governments and representatives of the reviewed states have clearly expressed the great potential they see in AI and autonomy, including for military purposes, they have also emphasized concerns over these technological developments. Challenges that have gained attention can be categorized broadly into legal, ethical and security-related ones.

Debates on **legal challenges** have centered on the question of whether weapon systems with autonomous functions could be used in compliance with International Humanitarian Law (IHL), more specifically the principles of distinction, proportionality and precautions in attack as well as the principle of military necessity. Yet, while some have expressed concerns that decreasing human control in the decision to use force would undermine or even violate IHL, other state delegations have argued that AI-infused technologies, possibly even LAWS, could strengthen IHL by increasing precision and preventing collateral damage.[13]

Ethical concerns have similarly been discussed by all of the reviewed states and it has been stressed that advances in AI and its application for both civilian and military purposes should not violate ethical principles. While some states have left this discussion in rather vague terms, others have drafted dedicated strategy documents on the ethical use of AI.

A third set of challenges having received much attention relates to **international security and geopolitics**. In this context, states have expressed the concern that advances in AI could exacerbate existing tensions, trigger new rounds of arms races and undermine strategic stability.[14] Also the risk that AI-enabled technologies could proliferate and become available to armed non-state actors including terrorist groups has been highlighted by several of the reviewed states.[15]

---

[11]   Airbus and FKIE Fraunhofer (2020). Two iPRAW members, namely Anja Dahlmann and Frank Sauer, are part of the forum's expert panel.

[12]   See Edmonds et al. (2021, 62ff.).

[13]   See e.g. USA (2018a, p. 4).

[14]   See e.g. Germany (2018); People's Republic of China State Council (2017).

[15]   See e.g. Germany (2018).

3. STRATEGIES, POLICIES, AND REGULATIONS

The following subsections provide an overview of strategies, policies and other regulations that either explicitly or implicitly apply to LAWS and their component parts, from development and procurement, to deployment and export controls. Most of these policies take a broader angle by addressing (military) AI and enabling technologies of machine autonomy in general. Overall, the mapping of national regulations demonstrates that there are already a number of measures in place, but that certain loopholes and gaps remain, deserving greater attention.

3.1. GENERAL STRATEGIES

All five states that were reviewed have adopted AI strategies in recent years. Yet, **only few consider AI in the context of national security and for military purposes**. As mentioned above, **Japan**'s and **Germany**'s AI strategies only focus on AI for civilian purposes.[16] The **EU Commission** also adopted an AI strategy in 2018 as well as a White Paper on AI in 2020, both of which only address AI in the civilian realm. Similarly, **Russia**'s strategy documents, including an AI roadmap as well as an AI strategy, center on civilian applications, especially for the economic sector.[17] Nevertheless, Russia's new "National Security Strategy" adopted in July 2021 also underlines the importance of advances in AI and robotics in the context of national security.[18]

In **China**, the State Council issued a "Development Plan on the New Generation of Artificial Intelligence" in 2017. While it addresses the use of AI more broadly, it lists national defense as an important area of AI research, development and application.[19] This is echoed in China's "National Defense White Paper" from 2019 underlining the

---

[16]   See Germany (2020); Japan (2019, 2021).

[17]   See Russian Federation (2019b); Russian Federation (2019a).

[18]   See Russian Federation (2021b).

[19]   See People's Republic of China State Council (2017).

development towards "intelligent…weaponry and equipment" and stressing that "intelligent warfare is on the horizon."[20]

In contrast to the other states reviewed in this report, in the **US,** the Department of Defense adopted a dedicated AI strategy in 2018 encouraging AI innovation for military purposes while highlighting the need to ensure that AI ethics and safety are adequately taken into consideration.[21]

All of these strategies reflect an acute awareness for the intensifying competition in the field of AI, a sense of urgency, and an ambition to be among the leading states developing AI technology.

Ethical considerations in the context of AI have also been subject to policy documents in several of the reviewed states. The **US** Department of Defense released "Ethical Principles for Artificial Intelligence" in 2020, stressing that AI applications must be responsible, equitable, traceable, reliable, and governable.[22] Similarly, the **EU Commission** published "Ethics guidelines for trustworthy AI" in 2019, the conclusions of which also informed its proposed regulatory framework on AI, released in 2021 (see below).[23] Albeit being focused primarily on civilian AI, the Commission's guidelines also address LAWS and endorse a ban thereof.[24] Both the US Department of Defense as well as the EU Commission relied on a multi-stakeholder approach when developing and formulating these principles, involving the private sector and civil society, including experts from academia. The **German** Federal Government set up an independent Data Ethics Commission in 2018 that developed ethical benchmarks and guidelines for data and algorithmic systems, including AI. The Data Ethics Commission took a similar stance on LAWS as the EU Commission's guidelines.[25] Similarly, the Ethics Committee of the **Japanese** Society for Artificial Intelligence issued ethical guidelines for AI in 2017, calling for responsible AI research.[26] Additionally, Japan's AI strategy also underlines the importance of an ethical and human-centric approach in the area of AI.[27]

Some of the countries have endorsed ethical considerations in their AI strategies or other policy documents. **Russia**, for example, addresses ethical norms in its "Concept for the development of regulation of relations in the field of AI and robotic technologies through 2024," published in 2020, and underlines the need for a human-centric approach to AI.[28] **China**'s "Development Plan on the New Generation of Artificial Intelligence" considers the development of "laws and regulations, ethical norms and

---

[20]   People's Republic of China State Council (2019).

[21]   See US Department of Defense (2018).

[22]   See US Department of Defense (2020c).

[23]   See High-Level Expert Group on Artificial Intelligence (2019); EU Commission (2021).

[24]   Furthermore, the European Parliament has adopted several resolutions on AI, i.a. on ethics and AI, see: European Parliament (2020).

[25]   See German Data Ethics Commission (2019, p. 180).

[26]   See Japan (2017).

[27]   See Japan (2021).

[28]   See Russian Federation (2020a).

policy systems" as important goals.[29] In 2019, China furthermore established a "National Ethics Committee on Science and Technology" which is supposed to advance regulations on dual-use technologies, including AI.[30]

KEY TAKEAWAYS & RECOMMENDATIONS

➢ Formulating clear policy documents and principles that address not only civilian but also military applications of AI is of utmost importance. Only considering one side of the coin – i.e. the civilian one – remains insufficient.

➢ This effort should go hand in hand with the determination of clear responsibilities and criteria to operationalize broader goals and principles from these strategies.

➢ Beyond that, as some of the case studies demonstrate, involving different stakeholders in the formulation of broader documents can prove valuable for considering distinct perspectives – a crucial aspect in light of the multiple purposes and use cases of (military) AI.

3.2. DEVELOPMENT & PROCUREMENT

In the development and procurement process of new weapon systems, weapon reviews are of particular importance. While Article 36 of Additional Protocol I to the Geneva Conventions of 12 August 1949 (AP I) has laid down an obligation for States Parties to conduct such reviews, the implementation and enforcement of the specific review process is undertaken at the national level. Therefore, several states have developed their own review mechanisms, although these processes differ in both content and scope. Of those countries that are covered in our case studies, Germany, Russia, China and Japan have ratified AP I.

As a party to AP I, **Germany** has been conducting respective weapon reviews for years. Nevertheless, against the backdrop of technological advances and their use for military purposes, in 2015 and 2016, it institutionalized a formal procedure for weapon reviews that determines processes, standards and responsibilities. The lynchpin of Germany's reviews are all rules and principles of IHL binding upon Germany. The review process only considers the usual and intended ways of utilization, meaning that not every possible option to use the system are under closer scrutiny.[31]

Japan is also a party to AP I and has indicated that it conducts weapon reviews in accordance with IHL. In a commentary to the GGE in 2020, Japan elaborated further that from its point of view "Article 36 can be interpreted as obligating each High Contracting Party, in its research, development, acquisition or adoption of a new weapon, means or method of warfare, to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of

---

[29] See People's Republic of China State Council (2017).

[30] See People's Republic of China (2021, pp. 2–3).

[31] See Bundestag (2016); Sohm (2018).

international law applicable to the High Contracting Party" and proposed to introduce an "implementation mechanism of weapons review into the annual report of the CCW."[32] Furthermore, Japanese Defense Minister Nobuo Kishi said in 2020 that the Ministry of Defense and the Self-Defense Forces "do not conduct research and development on equipment whose use is not authorized by international or domestic law."[33]

In a working paper for the GGE, **Russia** underlined that it considers the obligation to conduct weapon reviews according to Article 36 as a norm of customary international law. The Russian Federal Law No. 275-FZ of December 2012 "On the State Defense Order" regulates the conduct of tests of prototypes of military equipment. Russia further elaborated that "prototypes are assessed for such characteristics as distinction, 'no-excessive-damage', etc., which should guarantee potential compliance of future weapons with IHL norms."[34] Furthermore, the government standards GOST RV 15.203-2001 were adopted as guidance for industrial enterprises for the development of "special-purpose means (including the so-called prospective LAWS). For development of any new prototype, a list of normative guiding documents is made on the basis of operational requirements that necessarily include provisions on the need to comply with IHL norms and other applicable international legal obligations."[35]

China, on the other hand, has several regulations in place that direct testing and verification procedures of military equipment but do not refer to weapon reviews according to Article 36, despite China being a State Party to AP I.[36] These regulations include "Principles of New Generation Artificial Intelligence Governance-Responsible AI" that were released in 2019 and include the following eight principles on AI development: "Harmony and Human-friendly, Fairness and Justice, Inclusion and Sharing, Respect for Privacy, Safety and Controllability, Shared Responsibility, Openness and Collaboration, Agile Governance."[37] It remains unclear how these are being implemented in practice.

Even though the **US** has not ratified AP I, the Department of Defense's (DoD) Directive 5000.01 "requires that the acquisition and procurement of DoD weapons and weapon systems be consistent with all applicable domestic and international law, including the law of war."[38] Thus, as part of the acquisition process of a weapon system, a legal review has to take place. Also, DoD Directive 2311.01 determines that "[t]he intended acquisition, procurement, or modification of weapons or weapon

---

[32]   (Author's translation) Japan (2020, p. 3).

[33]   Kishi (2020).

[34]   Russian Federation (2020b).

[35]   Russian Federation (2020b, p. 6).

[36]   Examples are the PLA Regulations on the Research of Equipment from 2004; Provisions on the Management of the Quality of Military Software from 2005; Regulations on the Quality Control of Weapons Equipment from 2010. As several regulations are classified, it is not clear whether a regulation that directly refers to weapon reviews does exist.

[37]   People's Republic of China (2021, pp. 2–3).

[38]   USA (2017, pp. 1–2). See Directive: US Department of Defense (2020b).

systems is reviewed for consistency with the law of war" and sets out further measures and responsibilities.[39]

In addition, the Department's Directive 3000.09 released in 2012 and updated in 2017, establishes specific regulations to ensure the development of robust, reliable systems with autonomous functions.[40] Most importantly, Directive 3000.09 states that "[a]utonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[41] For this purpose, these systems are subject to rigorous testing, taking into account inter alia human-machine interfaces and controls. This includes legal reviews that are conducted before the development and again before deploying the weapon. Similar to the German regulations, also the US regulations only demand reviewing the intended and usual ways of utilization.

Despite the number of US regulations in place, a study mandated by the US Congress found that "[t]he current state of AI verification, validation, test, and evaluation (VVT&E) is nowhere close to ensuring the performance and safety of AI applications, particularly where safety-critical systems are concerned. Although this is not a problem unique to DoD, it is one that significantly affects DoD."[42] This assessment was echoed by several other reports.[43]

Several **EU institutions** have also developed positions and specific measures on the development of weapon systems with autonomous functions. In two resolutions, the European Parliament stressed that the need to retain human control should already be taken into account when designing and developing weapon systems.[44] The EU External Action Service endorsed this stance.[45] This approach has furthermore found its way into the mandate of the European Defence Fund (EDF). The EDF was set up in 2021 and is supposed to support collaborative actions and EU cross-border cooperation on defense products and technologies for the period until 2027. It is worthy of note that the EDF explicitly excludes the support for the development of such products or technologies that do not warrant human control over their critical functions.[46] Beyond that, the EU Commission put forward a proposed regulatory framework on AI in spring 2021. The proposal relies on a risk-based regulatory methodology, differentiating between unacceptable, high, low or minimal risk and requiring appropriate quality management and conformity assessment corresponding to these categories. In accordance with the powers and responsibilities of the EU, the

---

[39]   See (and read more about the different directives here): USA (2021a); US Department of Defense (2020a).

[40]   See US Department of Defense (2012, 2017).

[41]   US Department of Defense (2012, 2017).

[42]   Tarraf et al. (2019).

[43]   See Scharre (2021).

[44]   See European Parliament (2020); European Parliament (2021).

[45]   See EU (2019).

[46]   See European Parliament (2021); Brzozowski (2021).

proposal however states that "AI systems exclusively developed or used for military purposes" are excluded from the framework's scope.[47]

KEY TAKEAWAYS & RECOMMENDATIONS

> ➢ While several of the reviewed states have ratified AP I, the extent to which they have put in place processes and defined responsibilities for thorough weapon reviews differs. Therefore, sharing procedural approaches and best practices on weapon reviews in the area of AI-enabled technologies and machine autonomy by States Parties will help advance and give full effect to the obligations under Article 36.

> ➢ It would likewise be fruitful if those states and organizations that have put in place further regulations with repercussions for the development of LAWS and their enabling technologies, shared these practices, e.g. in the GGE deliberations.

> ➢ The current state of verification, validation, test, and evaluation (VVT&E) in the area of AI and machine autonomy is not deemed fit for purpose for safety critical systems, including military applications. In light of the unique character of enabling technologies in the area of LAWS, including software and data-driven methods, states should internally scrutinize their review criteria for such systems and their components, including the training data they rely on. Testing the reliability and predictability of such systems will require fundamentally different practices and criteria than those used for traditional weapon systems.

> ➢ In order to update and adapt their review processes, states could commission independent reviews of their current practices, relying on an interdisciplinary multi-stakeholder approach to involve various fields of expertise and perspectives.

3.3. DEPLOYMENT

At present, there are only few national regulations in place that directly address the deployment of weapon systems with autonomous functions. However, several international norms apply that have repercussions on national procedures and practices, namely IHL and ethical requirements. For now, national regulations on (remotely piloted) unmanned weapon systems would be relevant for weapon systems with increasingly autonomous functions, too,[48] but might have to be adjusted to explicitly regulate human control over the use of force.

In general, the **key principles of IHL**, i.e. the principles of distinction, proportionality, precautions in attack and military necessity, regulate the use of force in armed conflicts and would thus have implications for the deployment of autonomous

---

[47]   See EU Commission (2021).

[48]   See e.g. Germany Department of Defense (2020).

weapons. As these principles have assumed the status of customary international law, they apply to all states including those that have not ratified relevant humanitarian law treaties. Accordingly, the reviewed states also have procedures in place to educate and train military personnel about core IHL obligations.[49]

Furthermore, a principle of particular significance in the context of autonomous targeting is **human dignity**. This principle has been enshrined in international law and numerous national legislations, e.g. Article 1 of the German constitution. It is important to emphasize that the concept of human dignity may also have significant repercussions on targeting decisions. Christof Heyns, former UN Special Rapporteur on extrajudicial, summary or arbitrary executions, has argued that killing in war must not be arbitrary, meaning that it must be justified and must therefore have reasons to justify it.[50] Moreover, the decision to use lethal force must be taken with justification and reason. In the context of LAWS and autonomous killing, the question arises whether a calculated machine decision, i.e. computations based on sensor data, can meet these criteria.[51]

Beyond that, some states adopt **rules of engagement** based on IHL and other legal norms that must be considered when deploying weapon systems. Information on this matter remains however limited. The US stated at the GGE in 2018 that "[t]he lawful use of force is context dependent and a human must authorize such use of force against an appropriately targeted objective. With all weapons systems, the commander's authorization is made within the bounds established by the rules of engagement and international humanitarian law (IHL) based on: a.) The commander's understanding of the tactical situation, informed by [his or] her training and experience. b.) The weapon's system performance, informed by extensive weapons testing as well as operational experience; and c.) The employment of tactics, techniques, and procedures for that weapon. In all cases, the commander is accountable and has the responsibility for authorizing weapon release in accordance with IHL."[52] Additionally, the US DoD's Directive 3000.09 comprises regulations on the deployment of weapon systems with autonomous functions. Most importantly, it states that "[p]ersons who authorize the use of, direct the use of, or operate autonomous and semi-autonomous weapon systems must do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement (ROE)."[53]

---

[49]   See Germany Department of Defense (2019); ICRC ; Russian Federation Ministry of Defence (2020); Russian Federation (2021a); Wenjuan and Chen, Kelly [trans.] (2013); People's Republic of China Ministry of Foreign Affairs (2010).

[50]   See Heyns (2013).

[51]   This section is partly based on iPRAW (2018, 11ff.).

[52]   USA (2018b, p. 1).

[53]   US Department of Defense (2012, 2017).

KEY TAKEAWAYS & RECOMMENDATIONS

➢ At this stage, there are only few regulations in place that govern the deployment of LAWS. Most of them address the use of weapon systems with autonomous functions only indirectly. This may lead to distinct views on the use of LAWS and diverging deployment practices.

➢ Therefore, it would be beneficial for states to work towards a similar understanding around the question of deploying systems with autonomous functions, exchange best practices on rules of engagement and the training of operators and commanders. Creating international norms on the (development and) use of LAWS would also leave less decisions at national discretion, making it less susceptible to changes in national policies and rules of engagement.

➢ Creating international norms on the deployment of LAWS could also help to create a more stable legal architecture potentially reducing the risk of escalatory dynamics in conflicts.

3.4. EXPORT

The states under review here generally differentiate between the export of items with explicit defense purposes and dual-use technologies. These categories are usually subject to different export licensing processes with distinct bodies responsible for issuing such licenses. Most of the components that could be used to build autonomous weapons fall under the category of dual-use items in the different countries. Several states have recently updated their export control regimes. **Yet, most of them are only beginning to grapple with fully incorporating enabling technologies in the area of LAWS into their export control regimes and several aspects remain unclear.** Thus, while hardware components are largely covered by the regulations, alongside technical information and certain software related to these, loopholes and grey areas in regulating intangibles remain.

China only recently adopted a new "Export Control Law" (ECL) entering into force in December 2020. The controlled items under the ECL include "dual-use items, military items, nuclear items, and other technologies, services and items related to the maintenance of national security, national interests and to the implementation of international obligations of anti-proliferation", as well as "technical information and other data related to the items."[54] Reportedly during the drafting process, it had been suggested that "source code and algorithms" should also be explicitly included in the controlled items, or to replace the wording "technical information and other data related to the items" with "technologies, information, and data."[55] It is unclear why the final text did not adopt these suggestions, but it raises questions about how broad the scope of "technical information and other data" is.

---

[54] National People's Congress of the Republic of China (2020, Art. 2).

[55] 21st Century Business Herald (2020)**.**

Also **Russia** has voiced its intention to adapt the Russian export control regime to incorporate AI technologies. The 2020 "Concept for the Development of Regulation of Relations in the Field of Artificial Intelligence and Robotics Technologies until 2024" stipulates in Section II.4 entitled "Improving the export regime for artificial intelligence and robotics systems" as follows: "In order to develop Russian projects in artificial intelligence and robotics technologies, it is necessary to create a favorable regime for their export. Export restrictive measures should only be applied in areas directly affecting national security interests."[56] The concept proposes an update of existing dual-use regulations to clearly govern the export of AI technologies and robotics.

For **EU** Member States, including Germany, the export, technical assistance, transit, transshipment and brokering of dual-use items, software and technology is regulated by the "EU Dual-use Regulation" which was most recently amended in December 2020. This regulation also takes into account international commitments of Member States, for example the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and the Missile Technology Control Regime (MTCR). Together with other national laws,[57] **Germany**'s export control regime largely covers components that could be used to build weapon systems with autonomous functions, including hardware, such as unmanned aerial vehicles (UAV), sensors as well as software. While these regulations generally comprise technical information related to these items, it is difficult to assess the extent to which training data for data-driven techniques are covered.

In recent years, the **US** has strengthened its export control regime on dual-use and emerging technologies, including those that could potentially be used in autonomous weapon systems. In 2018, the US introduced the Export Control Reform Act (ECRA), modifying the already existing US Export Administration Regulations (EAR). ECRA facilitates stricter controls on "emerging and foundational technologies [that are] essential to the national security of the United States."[58] Being responsible for export controls of dual-use technologies, the Department of Commerce's Bureau of Industry and Security (BIS) published an initial list of 14 categories of emerging technologies, proposing that these should be placed on the Commerce Control List (CCL).[59] The categories include inter alia AI and machine learning technology, advanced computing technology and robotics. Since its proposal, the BIS has awaited public comments and has not yet published a final list of emerging technologies that will be added to the CCL. In addition, in January 2020, the BIS imposed new export controls on AI software that is specially designed to automate the analysis of geospatial imagery. Reportedly, the US also plans to propose the rule in the framework of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies to internationalize it.[60]

---

[56] (Author's translation) Russian Federation (2020a).

[57] Such as the War Weapons Control Act (Kriegswaffenkontrollgesetz) and the External Trade and Payments Act (Außenwirtschaftsgesetz) in conjunction with the Foreign Trade Regulation (Außenwirtschaftsverordnung).

[58] US Congress (2018).

[59] See US Industry and Security Bureau (19.11.18).

[60] See Gibson Dunn (2021); SPIE (2020).

Beyond that, commercial and military UAV technologies are already part of US export control regulations.[61] Nevertheless, US export policies on UAV technologies have seen certain changes, pursued by the different administrations. The Obama Administration strengthened US export control law on UAV technologies and initiated a "Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled UAVs" with almost 50 other states.[62] Under the Trump Administration, the US, however, weakened to some extent these initiatives. This included declaring a unilateral reinterpretation of the MTCR regarding UAVs in the form of a national discretion, facilitating a more flexible export control treatment of heavy armed UAVs.[63] In March 2021, it was reported that the Biden Administration will not revoke this national discretion. Yet, reportedly, the Biden Administration will try to negotiate a new agreement only pertaining to the export of UAVs and will "work with other countries to shape international standards for the sale, transfer, and subsequent use of armed UAS [unmanned aerial systems]."[64]

KEY TAKEAWAYS & RECOMMENDATIONS

➢ As the analysis demonstrates, states are only beginning to adapt their export control regimes to the characteristics and requirements of enabling technologies in the area of LAWS. Focusing only on hardware - as traditional export control regimes primarily do - will however prove insufficient. At the same time, fundamental questions remain as to whether and how export control can be used and enforced to curtail effectively the proliferation of weapon systems with autonomous functions and their dual-use components.

➢ Therefore, independent studies should be undertaken that analyze whether and how export controls can be designed to grapple with the unique nature of software that is easily modifiable and could be used in the development of LAWS.[65] Importantly, this effort should not only be limited to data-driven techniques, such as machine learning, but consider the diffusion of software more broadly as various techniques and components can enable machine autonomy for military purposes.

➢ This should be complemented by international multi-stakeholder discussions on the design and use of export control in the area of military AI and machine autonomy. In this context, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies and potentially also the MTCR could prove as suitable fora.

---

[61] See lists here: USA (2021b); US Bureau of Industry and Security (2020).

[62] See US Department of State (2015); US Department of State (2016). See also: Jensen (2016).

[63] The MTCR is implemented through national policies, in the US case through § 742.5 of the EAR. See US Bureau of Industry and Security (2021); Stone (2021); Mehta and Insinna (2020).

[64] Stone (2021).

[65] A preliminary study indicates that the open source licensing is an inadequate approach for soft governance of open source software. See: Lin and Moon (2020).

4. CONCLUSION

This report has analyzed how states – specifically the US, Russia, China, Japan, and Germany in combination with the EU – approach technologies related to weapons with autonomous functions and which specific regulations are already in place.

Overall, the analysis has demonstrated that there are only few regulations in place that directly address LAWS. Instead, most policies and regulations cover aspects and enabling technologies of LAWS without directly considering weapon systems with autonomous functions. Additionally, several states have rather focused on regulating non-military applications of AI and have only briefly considered the issue of LAWS. Therefore, several key takeaways and best practices can be extracted from the analysis:

➢ The development of dedicated **strategies** and policies that consider military applications of AI and weapon systems with autonomous functions deserves further attention.

➢ A **multi-stakeholder approach** involving experts from civil society, including academia, and industry, can prove valuable when embracing and aligning different perspectives and formulating policies that are legal, ethical, practical and effective. As some states and organizations have relied on such approaches already, it might be valuable to exchange best practices on these efforts.

➢ The extent to which states have put in place substantive **weapon review mechanisms** differs greatly, allowing for distinct approaches to – and perhaps even deficiencies in – system safety and robustness. Cross-pollination of ideas and the sharing of best practices exercised across states on testing, evaluation and validation processes would be valuable. This should also entail knowledge exchanges on the special requirements for testing enabling technologies of LAWS.

➢ In light of the unique character of AI-based data-driven techniques and other technologies enabling machine autonomy, states should also scrutinize whether their **review criteria and verification, validation, test, and evaluation (VVT&E) practices** are fit for purpose when reviewing AI-enabled

systems and systems with autonomous functions, including the software and training data they rely on. Testing the reliability and predictability of such systems will require fundamentally different practices and criteria than those used for traditional weapon systems.

➢ At this stage, most regulations govern the **deployment** of LAWS only implicitly which may lead to distinct views on the use of LAWS and diverging deployment practices. Therefore, it would be beneficial for states to work towards a similar understanding around the question of and limitation for deploying systems with autonomous functions, exchange best practices on rules of engagement and the training of operators and commanders to safeguard human control.

➢ Fundamental questions remain as to whether and how **export controls** can be designed and enforced to curtail effectively the diffusion of weapon systems with autonomous functions and their dual-use components. Clearly, the hardware-based methodology of traditional export control regimes is insufficient for addressing the proliferation of technologies that enable machine autonomy for military purposes. Therefore, independent studies and dedicated international multi-stakeholder discussions could enhance the understanding of how export control can be rethought to address the unique nature of software and other enabling technologies of LAWS.[66]

Several of these steps would require individual states to review and update their policies. Especially when it comes to sharing best practices and experiences in regulating technologies in the area of LAWS, the GGE on LAWS would however prove as an adequate forum for such debates. For specific issues, other international fora could prove valuable as well, such as the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

National practices can shape the norms around the development and use of LAWS, contributing to the normative space in which a CCW Protocol might evolve or will be contested – e.g. human control in the use of force.[67] Therefore, it is important for the GGE to understand which national policies and regulations in the area of LAWS exist.

---

[66] For further considerations on export controls for LAWS and related technologies, see iPRAW (2020).

[67] See Bode and Huelss (2018).

5. LITERATURE

21st Century Business Herald (2020), 'Export Control Law Will Take Effect Since December: Source Code and Algorithms Were Included in Controlled Items in the Third Draft [21世纪经济报道：“《出口管制法》12月起实施：三审稿源代码和算法列入管制范围"]', *21st Century Business Herald*.

Airbus and FKIE Fraunhofer (2020), 'FCAS: Mission', accessed 22 February 2021, at www.fcas-forum.eu/en/mission/.

Anger, D. (2018), 'Microsoft Says It Will Sell Pentagon Artificial Intelligence and Other Advanced Technology', *The New York Times*.

BAAI (2019), 'Beijing AI Principles [人工智能北京共识]', accessed 21 June 2021, at www.baai.ac.cn/news/beijing-ai-principles.html.

Bode, I. and H. Huelss (2018), 'Autonomous Weapons Systems and Changing Norms in International Relations', *Review of International Studies,* **44**(3), 393–413.

Brewster, T. (2020), 'Google Promised Not To Use Its AI In Weapons, So Why Is It Investing In Startups Straight Out Of 'Star Wars'?'.

Browne, R. (2019), 'Alibaba's Jack Ma Suggests Technology Could Result in a New World War', *CNBC.*

Brzozowski, A. (2021), 'European Parliament backs EU's €7.9 billion defence fund', *EURACTIV.*

Bundestag (2016), *Zentrale Dienstvorschrift - Prüfung neuer Waffen, Mittel und Methoden der Kriegführung: Drucksache 18/9191.*

China IT News (2018), 'Li Yanhong unveiled after "Baidu lost the land": "Simple search" without advertisement, mass production of unmanned vehicles in July', accessed 21 June 2021, at www.firstxw.com/view/208592.html.

Edmonds, J., S. Bendett, A. Fink, M. Chesnut, D. Gorenburg, M. Kofman, K. Stricklin and J. Waller (2021), 'Artificial Intelligence and Autonomy in Russia', accessed 21 June 2021, at www.cna.org/centers/cna/sppp/rsp/russia-ai.

EU (2019), 'EU Statement Group of Governmental Experts Lethal Autonomous Weapons Systems Convention on Certain Conventional Weapons Geneva, 25-29 March 2019: Further consideration of the human element in the use of lethal force; aspects of human-machine interaction in the development, deployment and use of emerging technologies in the area of lethal autonomous weapons

systems', accessed 23 February 2021, at reachingcriticalwill.org/images/
documents/Disarmament-fora/ccw/2019/gge/statements/26March_EU5c.pdf.

EU Commission (2021), 'Proposal for a Regulation of the European Parliament and of
the Council laying down harmonized rules on Artificial Intelligence (Artificial
Intelligence Act) and amending certain Union legislative acts: COM(2021) 206
final / 2021/0106(COD)', accessed 1 July 2021, at eur-lex.europa.eu/legal-
content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

European Parliament (2020), 'European Parliament resolution of 20 October 2020 with
recommendations to the Commission on a framework of ethical aspects of
artificial intelligence, robotics and related technologies: (2020/2012(INL))',
accessed 1 July 2021, at www.europarl.europa.eu/doceo/document/TA-9-2020-
0275_EN.html.

European Parliament (2021), 'European Parliament resolution of 20 January 2021 on
artificial intelligence: questions of interpretation and application of international
law in so far as the EU is affected in the areas of civil and military uses and of
state authority outside the scope of criminal justice (2020/2013(INI)): P9TA-
PROV(2021)0009', accessed 25 January 2021, at www.europarl.europa.eu/
doceo/document/TA-9-2021-0009_EN.pdf.

Franke, U.E. (2019), 'Not Smart Enough: The Poverty of European Military Thinking
on Artificial Intelligence', ECFR, London, accessed 14 March 2020, at
www.ecfr.eu/page/-/Ulrike_Franke_not_smart_enough_AI.pdf.

Future of Life Institute (2021), 'Lethal Autonomous Weapons Pledge - Future of Life
Institute', accessed 21 June 2021, at futureoflife.org/lethal-autonomous-weapons-
pledge/.

German Data Ethics Commission (2019), 'Opinion of the Data Ethics Commission',
accessed 21 June 2021, at datenethikkommission.de/wp-content/uploads/DEK_
Gutachten_engl_bf_200121.pdf.

Germany (2018), 'Statement delivered by Germany on Security Dimension and
Options'.

Germany (2020), 'Artificial Intelligence Strategy of the German Federal Government:
Update', accessed 22 February 2021, at www.ki-strategie-deutschland.de/files/
downloads/Fortschreibung_KI-Strategie_engl.pdf.

Germany Department of Defense (2019), 'Regeln des Krieges: Humanitäres
Völkerrecht', accessed 8 July 2021, at www.bmvg.de/de/themen/
friedenssicherung/humanitaeres-voelkerrecht.

Germany Department of Defense (2020), 'Bericht des Bundesministeriums der
Verteidigung an den Deutschen Bundestag zur Debatte über eine mögliche
Beschaffung bewaffneter Drohnen für die Bundeswehr', accessed 23 February
2021, at www.bmvg.de/resource/blob/274160/
f5d26b7af1a024551e4aafc7b587a01d/20200703-download-bericht-
drohnendebatte-data.pdf.

Gibson Dunn (2021), '2020 Year-End Sanctions and Export Controls Update',
accessed 7 July 2021, at www.gibsondunn.com/2020-year-end-sanctions-and-
export-controls-update/.

Grünwald, R. and C. Kehl (2020), 'Autonome Waffensysteme: Endbericht zum TA-
Projekt, TAB-Arbeitsbericht Nr. 187', Büro für Technikfolgen-Abschätzung beim
Deutschen Bundestag (TAB), accessed 5 November 2020, at www.tab-beim-
bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab187.pdf.

Heyns, C. (2013), 'A/HRC/23/47: Report of the Special rapporteur on Extrajudicial,
Summary or Arbitrary Executions', United Nations General Assembly.

High-Level Expert Group on Artificial Intelligence (2019), 'Ethics Guidelines for Trustworthy AI', accessed 4 February 2021, at ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

ICRC, 'United States of America: 142. Instruction in International Humanitarian Law within Armed Forces', accessed 8 July 2021, at ihl-databases.icrc.org/customary-ihl/eng/docs/v2_cou_us_rule142.

iPRAW (2018), 'Focus on Ethical Implications for a Regulation of LAWS', Berlin, accessed 6 August 2019, at www.ipraw.org/wp-content/uploads/2018/08/2018-08-17_iPRAW_Focus-On-Report-4.pdf.

iPRAW (2020), 'LAWS and Export Control Regimes: Fit for Purpose?', Berlin, accessed 3 July 2020, at www.ipraw.org/wp-content/uploads/2020/04/iPRAW_WP_ExportControls.pdf.

iPRAW (2021), 'Building Blocks for a Regulation of LAWS and Human Control: Updated Recommendations to the GGE', accessed 18 August 2021, at www.ipraw.org/wp-content/uploads/2021/07/iPRAW-Report_Building-Blocks_July2021.pdf.

Japan (2017), 'AI Ethical Guidelines [人工知能学会 倫理指針]', accessed 13 August 2021, at www8.cao.go.jp/cstp/tyousakai/humanai/1kai/siryo3-4.pdf.

Japan (2019), 'AI Strategy 2019. AI for Everyone: People, Industries, Regions and Governments: Integrated Innovation Strategy Promotion Council Decision', accessed 14 July 2021, at www.kantei.go.jp/jp/singi/ai_senryaku/pdf/aistratagy2019en.pdf.

Japan (2020), 'Commentary on the operationalization of the Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems at national level', accessed 9 July 2021, at documents.unoda.org/wp-content/uploads/2020/09/20200828-Japan.pdf.

Japan (2021), 'AI Strategy 2021 - Follow-up to AI Strategy 2019 [AI 戦略2021 - 「ＡＩ戦略2019」フォローアップ]', accessed 13 August 2021, at www8.cao.go.jp/cstp/ai/aistrategy2021_honbun.pdf.

Japan Ministry of Defence (2020), 'Efforts to Make the Most Effective Use of Limited Human Resources [限られた人材を最大限有効に活用するための取組]', accessed 13 August 2021, at www.mod.go.jp/j/publication/wp/wp2019/html/n42102000.html.

Jensen, A. (2016), 'U.S. Seeks Rules for Armed Drones Trade | Arms Control Association', accessed 19 April 2021, at www.armscontrol.org/act/2016-10/news/us-seeks-rules-armed-drones-trade.

Kishi, N. (2020), 'The 203rd Diet Session, House of Representatives, Committee on Security No. 2, November 13, 2020 [第203回国会　衆議院　安全保障委員会　第2号　令和2年11月13日]', accessed 13 August 2021, at kokkai.ndl.go.jp/#/detail?minId=120303815X00220201113&spkNum=18&single.

Lin, C. and A. Moon (2020), 'Using Open Source Licensing to Regulate the Assembly of LAWS: A Preliminary Analysis', *2020 IEEE International Symposium on Technology and Society (ISTAS)*, 147–53.

Mehta, A. and V. Insinna (2020), 'Trump admin officially makes it easier to export military drones', *Defense News*.

National People's Congress of the Republic of China (2020), 'Chinese Export Control Law. [中华人民共和国出口管制法]', accessed 8 July 2021, at www.npc.gov.cn/npc/c30834/202010/cf4e0455f6424a38b5aecf8001712c43.shtml.

People's Republic of China (2021), 'China's Comments on the Working Recommendations of the Group of Governmental Experts on LAWS', accessed 2 July 2021, at documents.unoda.org/wp-content/uploads/2021/06/China.pdf.

People's Republic of China Ministry of Foreign Affairs (2010), 'PRC's First Report on the Implementation of the Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict. [中华人民共和国关于《儿童权利公约关于儿童卷入武装冲突问题的任择议定书》执行情况的首期报告]', accessed 8 July 2021, at www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/tyfg_674913/t812061.shtml.

People's Republic of China State Council (2017), 'The Development Plan on the New Generation of Artificial Intelligence (Development Plan) [新一代人工智能发展规划]', accessed 21 June 2021, at www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

People's Republic of China State Council (2019), 'White Paper on 'China's National Defence in the New Era'', accessed 8 July 2021, at www.xinhuanet.com/english/2019-07-24/c_138253389.htm.

RIA Novosti (2021), 'The Ministry of Defense will create a department for Artificial Intelligence [Минобороны создаст управление по искусственному интеллекту]', *RIA Novosti*.

Russian Federation (2019a), 'Roadmap for the Development of End-to-End Digital Technology. "Neurotechnology and Artificial Intelligence." [Дорожная карта развития «сквозной» цифровой технологии. "Нейротехнологии и искусственный интеллект"]', accessed 17 June 2021, at digital.gov.ru/ru/documents/6658/.

Russian Federation (2019b), 'Presidential Decree No. 490 of 10.10.2019. "On the Development of Artificial Intelligence in the Russian Federation" (together with the "National Strategy for the Development of Artificial Intelligence for the Period until 2030"): [Указ Президента РФ от 10 октября 2019 г. № 490. "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года")]', accessed 30 March 2021, at www.garant.ru/products/ipo/prime/doc/72738946/#1000.

Russian Federation (2020a), 'Order of the Government of the Russian Federation of August 19, 2020 N 2129-r. Concept for the development of regulation of relations in the field of artificial intelligence and robotics until 2024: [Распоряжение Правительства РФ от 19.08.2020 N 2129-р. Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года]', accessed 21 June 2021, at d-russia.ru/wp-content/uploads/2020/08/0001202008260005.pdf.

Russian Federation (2020b), 'Working Paper of the Russian Federation: National Implementation of the Guiding Principles on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems', accessed 21 June 2021, at documents.unoda.org/wp-content/uploads/2020/09/Ru-Commentaries-on-GGE-on-LAWS-guiding-principles1.pdf.

Russian Federation (2021a), 'Federal Law of 29.12.2012 N 275-FZ (ed. from 30.04.2021) "On the State Defence Order" (as amended and supplemented, in force since 30.06.2021). [Федеральный закон от 29.12.2012 N 275-ФЗ (ред. от 30.04.2021) "О государственном оборонном заказе" (с изм. и доп., вступ. в силу с 30.06.2021)]', accessed 8 July 2021, at www.consultant.ru/document/cons_doc_LAW_140175/d937eace916904e588891489289ffc3063adc66c/.

Russian Federation (2021b), 'Presidential Decree of 02.07.2021 No. 400 "On the National Security Strategy of the Russian Federation": [Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации"]', accessed 8 July 2021, at publication.pravo.gov.ru/Document/View/0001202107030001.

Russian Federation Ministry of Defence (2020), 'Basic Provisions of International Humanitarian Law. [Основные положения международного гуманитарного права]', accessed 8 July 2021, at army.ric.mil.ru/Stati/item/259956/.

Scharre, P. (2021), 'Debunking the AI Arms Race Theory', *Texas National Security Review,* **4**(3).

Shanghai Municipal Science and Technology Commission (2019), 'Chinese Young Scientists' Declaration on the Governance and Innovation of AI [上海科技党建-创新人工智能治理，青年科学家发声《上海宣言》]', accessed 21 June 2021, at www.shkjdw.gov.cn/c/2019-08-30/517552.shtml.

Sohm, S. (2018), 'Die Zulassung neuer Waffensysteme', *Journal of International Law of Peace and Armed Conflict,* **1**(1-2), 19–27.

SPIE (2020), 'Export Control on Artificial Intelligence Software May Have Unintended Consequences', accessed 7 July 2021, at spie.org/news/photonics-focus/mayjun-2020/export-control--on-artificial-intelligence-software-may-have-unintended-consequences?SSO=1.

Stone, M. (2021), 'Exclusive: Biden wants to keep Trump policy that boosted armed drone exports - sources', *Reuters Media*.

Tarraf, D.C., W. Shelton, E. Parker, B. Alkire, D. Gehlhaus, J. Grana, A. Levedahl, J. Leveille, J. Mondschein, J. Ryseff, A. Wyne, D. Elinoff, E. Geist, B.N. Harris, E. Hui, C. Kenney, S. Newberry, C. Sachs, P. Schirmer, D. Schlang, V.M. Smith, A. Tingstad, P. Vedula and K. Warren (2019), *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*: RAND Corporation.

Tencent Research Institute (2021), '"ARCC": An Ethical Framework for Artificial Intelligence', accessed 21 June 2021, at www.tisi.org/13747.

The Indian Express (2017), 'Alibaba Chairman Jack Ma Thinks Artificial Intelligence Could Lead to World War III', *The Indian Express*.

US Bureau of Industry and Security (2020), 'Commerce Control List (CCL)', accessed 23 June 2021, at www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.

US Bureau of Industry and Security (2021), 'Change to the License Review Policy for Unmanned Aerial Systems (UAS) To Reflect Revised United States UAS Export Policy', accessed 19 April 2021, at www.federalregister.gov/documents/2021/01/12/2020-27983/change-to-the-license-review-policy-for-unmanned-aerial-systems-uas-to-reflect-revised-united-states.

US Congress (2018), 'H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019', accessed 16 April 2021, at www.congress.gov/bill/115th-congress/house-bill/5515/text.

US Department of Defense (2012, 2017), 'Directive 3000.09', accessed 28 July 2019, at www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.

US Department of Defense (2018), 'Summary of the 2018 Department of Defence AI Strategy: Harnessing AI to AdvanceOur Security and Prosperity', accessed 16 March 2021, at media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

US Department of Defense (2020a), 'DOD Directive 2311.01: DoD Law of War Program', accessed 2 July 2021, at www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101p.pdf?ver=2020-07-02-143157-007.

US Department of Defense (2020b), 'DoD Directive 5000.01: The Defense Acquisition System', accessed 17 June 2021, at www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500001p.pdf?ver=2020-09-09-160307-310.

US Department of Defense (2020c), 'DOD Adopts Ethical Principles for Artificial Intelligence', at www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

US Department of State (2015), 'U.S. Export Policy for Military Unmanned Aerial Systems', accessed 19 April 2021, at 2009-2017.state.gov/r/pa/prs/ps/2015/02/237541.htm.

US Department of State (2016), 'Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)', accessed 19 April 2021, at 2009-2017.state.gov/r/pa/prs/ps/2016/10/262811.htm.

US Industry and Security Bureau (19.11.18), 'Review of Controls for Certain Emerging Technologies: A Proposed Rule by the Industry and Security Bureau', accessed 21 June 2021, at www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

USA (2017), 'Autonomy in Weapon Systems: CCW/GGE.1/2017/WP.6', accessed 15 April 2021, at undocs.org/en/CCW/GGE.1/2017/WP.6.

USA (2018a), 'Humanitarian Benefits of Emerging Technologies in the Area of Lethal Autonomous Weapon Systems: CCW/GGE.1/2018/WP.4', accessed 28 July 2019, at reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/documents/GGE.1-WP4.pdf.

USA (2018b), 'U.S. Statement on the Human Element in the Use of Force', accessed 16 April 2021, at reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/statements/11April_US.pdf.

USA (2021a), 'Documents Reflecting U.S. Practice Related to Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.', accessed 2 July 2021, at documents.unoda.org/wp-content/uploads/2021/06/United-States-submission-on-national-practice.pdf.

USA (2021b), 'Electronic Code of Federal Regulations (eCFR): Part 121 - The United States Munitions List', accessed 23 June 2021, at www.ecfr.gov/cgi-bin/text-idx?node=pt22.1.121.

Wenjuan, W. and Chen, Kelly (2013), 'The PLA and International Humanitarian Law: Achievements and Challenges', *Asia Paper*.

MEMBERS OF IPRAW

Peter Asaro
Professor
The New School
New York, USA

Thompson Chengeta
European Research Council
Fellow on AI Ethics and
Drone Violence,
University of Southampton

Anja Dahlmann
Researcher, Head of Project
*German Institute for
International and Security
Affairs*
Berlin, Germany

Marcel Dickow
German Environment Agency
Dessau/ Berlin, Germany

Denise Garcia
Professor
Northeastern University
Boston, USA

Erin Hahn
Senior National Security
Analyst
*Johns Hopkins University
Applied Physics Laboratory*
Washington D.C., USA

**Elisabeth Hoffberger-
Pippan**
Researcher
*German Institute for
International and Security
Affairs*
Berlin, Germany

Vadim Kozyulin
Researcher
PIR Center for Policy Studies
Moscow, Russia

Ian MacLeod
Researcher
*Johns Hopkins University
Applied Physics Laboratory*
Washington D.C., USA

AJung Moon
Assistant Professor
McGill University
Montreal, Canada

Heigo Sato
Professor
Takushoku University
Tokyo, Japan

Frank Sauer
Senior Research Fellow
Universität der Bundeswehr
Munich, Germany

Lydia Wachs
Research Assistant
*German Institute for
International and Security
Affairs*
Berlin, Germany

Kelvin Wong
Unmanned Systems Editor
*Jane's International Defence
Review*
Singapore

Binxin Zhang
International lawyer and PhD
scholar in Political Science
Sciences Po
Paris, France