The Hague
Centre for
Strategic
Studies

HCSS Security

Effective Stakeholder Cooperation during the lifecycle of Robotic and Autonomous Systems

Bianca Torossian, Frank Bekkers & Klaudia Klonowska

Table of Contents

Introduction

It is commonly accepted that armed forces cooperate with external actors, outsource the production of arms, and share Research & Development projects with private companies and universities. Even though this practice is long-standing, the emergence of Robotic and Autonomous Systems (RAS) poses new questions and challenges to the effectiveness of multi-stakeholder cooperation in a military context. RAS are unique in that they ultimately can take humans 'out of the loop'[1] and, as a consequence, drastically affect operational performance, organizational embedding (e.g. influencing numbers, skills and training of personnel), operational concepts (i.e. doctrine and tactics), and raise specific ethical and regulatory concerns. In short, the introduction of a new RAS in the armed forces is seldom a 1-1 replacement of a more human-centric solution or a seamless fit to an identified capability gap. The nature of RAS intervention is disruptive and therefore renders the interaction between stakeholders more complex.

This paper studies the emerging complexity of relations between a wide variety of stakeholders involved in the development, integration and use of military RAS. The focus lies specifically with the interactions between the military and private parties, i.e. industry, knowledge institutes, and civil society (although the role of the national and international policy makers in this process is also acknowledged). Based on the findings, best practices are outlined and key requirements to improve the effectiveness of cooperation are highlighted through organizational, legal, and practical solutions.[2]

This paper is organized in the order of basic system life cycle stages: (1) development, (2) integration (transfer of ownership, organizational embedding), and (3) use of RAS in an operational environment. However, the specific nature of RAS often results in a Concept Development & Experimentation (CD&E) process, in which successive phases of development, acquisition, initial introduction, and use form a spiral development process (see Figure 1).

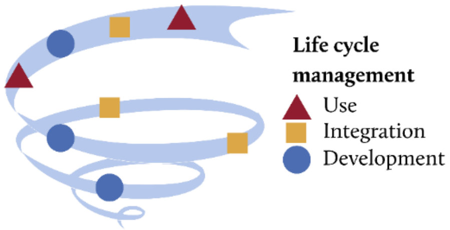

Figure 1: Spiral development process and the reoccurring stages of the system life cycle.

During the development and integration phases, concept development and testing of successive prototype versions go hand-in-hand to mature the system, potentially

[1] The scale from human 'in the loop, 'on the loop', to 'out of the loop' refers to the degree to which a human is involved in the operating and/or decision-making process of the system.

[2] The analysis provided in this paper is the result of an analysis of relevant literature, strengthened by insights from the expert session held by The Hague Centre for Strategic Studies on the 13th of February 2020. This session gathered an interdisciplinary group of professionals representing the government, businesses, and knowledge-institutes. Insights from the session are integrated throughout the paper.

including regular revisions of system requirements. During the use phases, lessons are learned that may retrospectively influence the functionality and design of a system, thereby requiring (potentially radical) updates. This iterative process blurs the distinction between each phase, as well as the lines between the developer/producer of the system on the one hand, and the defense organization as customer and user on the other. Instead of a definite hand-over in terms of ownership, responsibilities and liabilities, the various stakeholders are typically involved and interconnected throughout all stages of the RAS life cycle. Therefore, this paper also discusses the overarching issues and solutions under the heading of 'RAS life cycle management'.

Accordingly, chapter 1 outlines key differences between multi-stakeholder cooperation with RAS and other military technologies; chapters 2 to 4 discuss in further detail requirements of cooperation at each stage of the RAS life cycle, that is, development, integration and use; while chapter 5 provides a discussion of the overarching requirements for the so-called 'life cycle management'. The concluding chapter provides recommendations for effective and continuous cooperation between various stakeholders working with RAS in the military context.

1. Distinct cooperation challenges for RAS

There are a number of elements that make the development, introduction and use of RAS—and the stakeholder interactions that come with it—different from more traditional (linear) capability development processes:

- The development of RAS is to a great extent driven by civilian innovation, thus creating demands for interaction with designers, developers, and manufacturers outside the traditional defense industry;[3]

- Due to a rapid cycle of innovation within e.g. artificial intelligence (AI), RAS must be developed and acquired in fast-paced procedures, used for shorter periods of time, and modified, updated, inserted, or exchanged throughout the life cycle;

- The ethical questions and legal uncertainties surrounding the use of unmanned and increasingly autonomous systems demands interaction with a range of stakeholders and policy makers external to defense organizations;

- The fundamental changes that RAS might bring to (some or all of) the DOTMLPF-elements[4] requires broad interaction with stakeholders within the defense organization, with international military partners, and possibly with other partner agencies.

[3] Traditionally, technological innovation has emanated from the military-industrial complex. These innovations would later find civilian applications (known as the spin-off effect). In the case of RAS, as for other military systems that derive a large part of their functionality from information technology, the trend goes in the reverse direction (spin-in). Verbruggen, "The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems," 338–42.

[4] Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities. See, for example, https://military.wikia.org/wiki/DOTMLPF.

These distinct characteristics, risks, and opportunities associated with RAS give rise to specific requirements for cooperation between the armed forces and non-military partners to ensure effective development, integration and use of RAS.

2. Development

The development of RAS is a dynamic process of hardware and software design and production, which at later stages is consistently revisited according to the results of system testing, integration, monitoring, and use. It is increasingly more common for military forces to outsource the development of technologies to private actors in order to acquire unique expertise and skills needed for the development of sophisticated equipment such as RAS.[5] Innovations and a rapid growth in the public sector in the use of unmanned and increasingly autonomous systems (e.g. medical robots, autonomous vehicles, and an abundance of civil drones) inspire the adaptation of civil platforms for specific military purposes.[6] Thus, it can be said that RAS in the military context is developed in a 'spin-in' environment, whereby the civil domain leads in innovation. This chapter outlines solutions to improve the effectiveness of cooperation in this dynamic environment during the development of RAS.

2.1. Integrated and interdisciplinary cooperation

The first step in envisioning an effective cooperation throughout the lifecycle is to establish a suitable stakeholder cooperation at the initial phase of RAS development. RAS development demands the involvement of an increasingly interdisciplinary and long-term approach to stakeholder cooperation. Studies show that numerous states have already conducted interdisciplinary RAS-related projects in cooperation with industrial consortiums, universities, laboratories, and start-ups.[7] Interdisciplinary teams promise to meet the demand to adequately converge 'technical' and 'conceptual' requirements due to the integration of knowledge of actors with military experience on the one hand, and technical skills on the other. Additionally, it is desirable for knowledge institutes to be involved at this stage to provide out-of-the-box insights and for civil society to highlight possible ethical concerns. Cooperation at this stage should be extended and, where possible, well-integrated throughout the entire life cycle.

2.2. Division of tasks, investments and responsibilities

Cooperation between and co-creation of various stakeholders requires managing where responsibilities lie. One way to manage the extent of private actor involvement in RAS development is through contracting. The military should carefully consider how to establish a long-term relationship with the RAS developer/producer that will extend into other stages of the RAS life cycle on the one hand, and the ability to change partnership in case of ill-performance on the other. Under the typical co-creation conditions of CD&E, questions like 'who does what', 'who pays for what' and 'who bears

[5] Slijper, Beck, and Kayser, "State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons."
[6] Perlo-Freeman and Sköns, "The Private Military Services Industry," 4; Verbruggen, "The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems."
[7] Slijper, Beck, and Kayser, "State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons."

responsibly for what' do not always have a clear-cut answer. Contractual arrangements with built-in flexibility may provide guidance.

Cooperation with other countries further exacerbates the above-mentioned need to clearly divide tasks, investments, and responsibilities in RAS development. With the increase of contractors in the development and production of RAS, there are further difficulties in ensuring adequate design, oversight, and quality. Possible challenges include inconsistent communication (e.g. incoherent testing results may result in faulty design), lack of independent reviewers, or misleading political agendas. Effective solutions require political authorities and armed forces to harmonize requirements through, for example, tailored Memoranda of Understanding and international legal instruments.[8]

2.3. System architecture

The effectiveness of RAS depends greatly on the ability to communicate and share information with other sensors in order to collect and process real-time events in a dynamic environment.[9] Additionally, the ability of the military to respond and mitigate risks is dependent on the design of interface. From the technical perspective, this requires that the developer is progressive and can provide the most advanced solutions to create "easier, safer, and more flexible" systems.[10] From the military perspective, the chosen architecture must ensure that RAS can communicate with systems of other units or other countries in order to provide interoperability.[11] Common system architecture entails trusted intelligence sharing when cooperating with friendly forces, and security of information to prevent data exploitation by adversary forces. The choices made regarding the system architecture fundamentally influence the RAS (inter)operability, thus cooperation between all parties is required in order to pose and answer adequate questions.[12]

Besides interoperability, another consideration for the army is the ability to insert new RAS into the already existing platform-based systems. Changing demands of the army require that systems have modular and flexible architecture that can "facilitate the insertion of independently developed 'best-of-breed' cognitive functionality".[13] In order for the developer to respond to these challenges, it is necessary for them to know in advance what the current state-of-the-art of military systems are and what (future) demands need to be met.

[8] Clarke, "The Arrow Missile: The United States, Israel and Strategic Cooperation," 478.

[9] Kortenkamp and Simmons, "Robotic Systems Architectures and Programming," 188; "Robotic and Autonomous Systems of Systems Architecture," 38–39.

[10] Kortenkamp and Simmons, "Robotic Systems Architectures and Programming," 202.

[11] "Robotic and Autonomous Systems of Systems Architecture," 37.

[12] For the type of questions that relate to the system architecture both from the technical and organizational perspectives, see Kortenkamp and Simmons, "Robotic Systems Architectures and Programming," 202–3.

[13] "Robotic and Autonomous Systems of Systems Architecture," 37.

2.4 Matching 'pull' and 'push' factors

Matching military requirements with technological possibilities in a situation where both are moving targets presents a challenge. Military users and technical developers have different frames of reference and must therefore collaborate closely to ensure proper translation of military demands into technical parameters (and vice versa) in an ongoing spiral development process. Effectively balancing military requirements and expectations, technological possibilities, and (potentially conflicting) legal, ethical and safety parameters, is a requirement that all involved stakeholders must manage in order to facilitate cooperation.

3. Integration

Integration concerns the organizational embedding of mature RAS, of systems that are selected to be scaled-up from an experimental setting to the structural use. At this stage, the relationship with the developer/producer of the system changes and new actors, such as the actual military end-users, emerge or acquire a more dominant role. During this stage, the nature of 'hand-over' changes and raises new questions regarding the role of each actor. This chapter highlights the changing nature of integration of systems in the military context and proposes ways to enhance multi-stakeholder cooperation.

3.1. 'Hand-over' of military systems

The integration stage includes a type of 'hand-over' from the developer/producer to the military. However, a feature of RAS is the dependency upon integrated software that continuously evolves; certainly, where self-learning algorithms are part of the autonomous reasoning of the system. As a result, the hand-over of RAS does not necessarily finalize the involvement of the producer in the latter stages of the life cycle. The responsibility is likely to extend for the producer to ensure that the system is adequately and regularly updated, and that the self-learning nature of the system is controlled and continues to meet demands and standards. If the changes made by self-learning algorithms lead to alterations in the use of a system, this should be well explained to the operator prior to the first use after an 'update'.

Therefore, the hand-over of the system should be accompanied with a clear division of future responsibilities and liabilities, as well as the accountability for system failures, servicing, and software updates. A proposed alternative to the traditional hand-over of ownership is the licensing model or the service model, in which the developer/producer remains the owner of the system. Though licensing agreements may set strict criteria to guarantee the safety of a system, concerns may be raised regarding their exclusive ownership and control by private actors, since conflicts of interest can arise between the efficiency of the systems on one hand and national security or public safety on the other.

3.2. Testing environment

It is evident that all military equipment needs to be tested in order to provide quality assurance. In the case of RAS, it is particularly important to ensure that the system is tested in an environment that reflects, as close as possible, the intended operational environment. In order to meet the demands, it is desirable for a military end-user to have the opportunity to interact with the system and its interface in order to better understand the (autonomous) functionalities, its limitations and possibilities, and to develop a sense of trust in the system. Observations gathered from such an exercise, when conducted in collaboration with the developers, are likely to yield new upgrades in the system.

3.3. Comprehensive integration

The integration of RAS into military forces requires adaptation of processes beyond the units where RAS are deployed. It involves the adaptation of all the 'DOTMLPF' categories.[14] The military should consider whether the doctrine covers situations of RAS deployment, whether the training and organization of forces are sufficient to ensure that RAS are taken full advantage of, whether there is sufficient technical literacy to deal with ad-hoc technical problems, whether the facilities are equipped to repair RAS, etc. These questions should be answered during the integration stage in cooperation with actors that are involved in the development, *as well as*, with the end-users.

4. Use

The use stage of RAS involves the deployment, maintenance, and service of RAS. The use of RAS in operational environments fundamentally influences the ways in which the military work: how it conducts missions, with whom and under what conditions. Among others, this fundamental change can be attributed to operators and commanders interacting with the system at "higher levels of abstraction".[15] Specific solutions to improve cooperation between stakeholders at this stage are outlined below.

4.1. Human-machine teaming

RAS are typically deployed as part of mixed human-machine teams. Soldiers and RAS work alongside under high-demand circumstances, with mutual trust as a condition *sine qua non*. Personnel working with and alongside RAS in actual operations must be willing to adapt to changing circumstances and improve the understanding of and trust in system functionalities before deployment. Their tasks should be clearly divided to determine which team members are responsible for the validation of targets and have the control to override the decisions of the system. A clear division of responsibilities helps to reduce automation bias, promotes compliance with international legal obligations and principles, ensures human intervention, and prevents mode confusion (a situation when operators erroneously switch between highly- and less-automated modes).[16]

After use of RAS in an operational environment, it is important to reflect upon ways in which the system aided the operation, as well as failures to add value to mission

[14] Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities. See, for example, https://military.wikia.org/wiki/DOTMLPF.

[15] Platts, Cummings, and Kerr, "Applicability of STANAG 4586 to Future Unmanned Aerial Vehicles," 2.

[16] Platts, Cummings, and Kerr, 12.

objectives. An integrated process of feedback and improvement aids the culture of 'shared risk', whereby responsibilities, interests, and values are shared among stakeholders. Considerations from this stage of evaluation should be communicated to relevant stakeholders and/or to personnel that interact with similar RAS in other operational environments.

4.2. Continuous technology insertion

Since the development of, for example, AI-related technologies is fast-paced, RAS requires a (relatively) rapid update and upgrade cycle to stay relevant and competitive. Therefore, besides regular service and maintenance of RAS, third parties may continue to be involved in the re-configuration, updating, and upgrading of system functions after deployment.[17] Collaboration with stakeholders should be logically integrated in order to ensure that RAS upgrades continue to meet the demands of the military, are clearly understood and trusted by operators and other relevant personnel, and incorporate feedback provided from previous deployments. If necessary, from the upgraded system functionalities, military personnel should receive additional training to ensure their ability to interact with the system.

4.3. Security

RAS face specific operational security challenges, both in terms of intentional cyber/data breaches as well as unintentional failures. Parallel to the development of RAS, there are actors advancing capabilities to intercept, disrupt, jam, spoof, and hack communications of robotic systems.[18] Additionally, RAS relying on data that is stored remotely poses new risks to the management of sensitive data.[19] Even with cryptography providing new ways to encrypt data while maintaining confidentiality and integrity of information,[20] new questions arise of control over sensitive data and related infrastructure. Further efforts are necessary to provide military personnel and relevant partners with adequate cyber awareness trainings specific to the additional risks associated with the use of RAS.[21] Due to the greater level of technical understanding of system amongst the developers, it is desirable for private actors to inform the military about the requirements for effective use of their systems.

At the same time, the use of RAS may lead to unintentional safety issues. The machine learning techniques embedded in RAS may result in unpredictable and harmful accidents, due to an incorrect specification of functional objectives, inconsistent oversight over the learning process or other implementation errors.[22] It has been proven that even the most careful designs of automation known to us today may lead to 'system

[17] Kortenkamp and Simmons, "Robotic Systems Architectures and Programming."
[18] "The U.S. Army: Robotic and Autonomous Systems Strategy," 15.
[19] Bromley and Maletta, "The Challenge of Software and Technology Transfers to Non-Proliferation Efforts"; Allen and Chan, "Artificial Intelligence and National Security."
[20] Allen and Chan, "Artificial Intelligence and National Security," 91.
[21] "Army Cyber Training and Education within Finabel Member States," 11 (Pre-mission cyber awareness refers to the understanding of cyber threats within a specific new environment as well as other permanent threats such as social media.).
[22] "Safety, Unintentional Risk and Accidents," 3.

accidents'.[23] It is desirable for the military to continue cooperating closely with the initial designers of RAS in order to monitor and correct for system redundancy, automation bias, and neglectful responses.[24] An incentive-based scheme (similar to insurance schemes that reward safe behavior) may be used to reward the designers for implementing risk aversion measures.[25] The implementation of these so-called 'fail-safe' measures may help to mitigate unintended risks. Furthermore, it is important to remember that safety of RAS depends on the extent of system unpredictability, which in turn depends upon the extent of allowed automation in military technologies by the political authorities. Therefore, in order to mitigate the risks of RAS, it is necessary to keep an open and informative dialogue with the political decision-makers.

5. Life cycle management

As previously stated, the development, integration and use of RAS is not linear due to its evolving nature which requires an iteration of military requirements, review of technical parameters and regular adjustments to allow for technological progress and new operational insights to be reflected in the system and its actual use. This spiral development process typically requires long-lasting and multifaceted relationships between the developer/producer and the military user. The dependency that arises consequently calls for effective arrangements between the parties involved that include the entirety of the life cycle. Accordingly, the following requirements are particularly relevant to the life cycle management of RAS.

5.1. Meaningful oversight over stakeholders

The distinct nature of RAS raises regulatory and ethical questions. Studies have indicated a difficulty in determining accountability and liability for the wrongdoings caused by RAS.[26] With a greater number of actors involved, additional measures are necessary to ensure the line of accountability is clearly defined. This is particularly salient when cooperating with private companies, as this interaction increases the 'distance' between the decision-making and the operational behavior (potentially including the use of force). Even subtle differences in the design of a system may have critical consequences on the ways that RAS behave or the military interacts with RAS in an operational environment.[27] The notion of accountability is challenged when private entities are involved since RAS operate based on the parameters and functions set by private actors, and international law is centered around the principle that states alone have "the exclusive legitimacy to exercise violence".[28]

Thus, the military should exercise meaningful oversight over all stakeholders, including private contractors, in order to ensure the implementation of relevant legal restrictions

[23] "Safety, Unintentional Risk and Accidents," 3.
[24] "Safety, Unintentional Risk and Accidents," 12.
[25] See Wasiak, "What Is the Incentive in Insurance Premiums?"
[26] Chavannes, Klonowska, and Sweijs, "Governing Autonomous Weapon Systems."
[27] Chavannes and Arkhipov-Goyal, "Towards Responsible Autonomy: The Ethics of Robotic and Autonomous Systems in a Military Context," 19.
[28] Perlo-Freeman and Sköns, "The Private Military Services Industry," 13.

and ethical considerations specified either in international or domestic instruments. The basis of such oversight mechanisms can take a variety of forms, from internal guidelines, to codes of conduct and external harmonized international NATO frameworks, and should always be accompanied by communication mechanisms in order to ensure adequate interpretation and application.

5.2. Non-proliferation

The difficulty of adequately regulating RAS proliferation is further exacerbated by the large quantity of actors involved in the RAS life cycle. There is a possibility that private companies may re-sell or re-use RAS after the expiration of the contract or that states may transfer RAS elements to third countries without the approval of production partners.[29] There is a need for states to prevent proliferation of RAS and its elements by external partners beyond the established cooperation; for example, to ensure that the period of non-engagement is respected and the success of the project, and ultimately national security, are not endangered.

5.3. Collaborative engagement

An important requirement that may not be easily translated in contractual terms or technical parameters, but is nevertheless critical to an effective cooperation, is the creation of the so-called 'Formula 1 mindset'. The F1 mindset refers to a common sense of urgency shared by a diverse team that orients itself toward a clearly defined goal. A Formula 1 racing team is not only about the driver at the forefront of all the attention, it is about the way in which the whole team collaborates to achieve a shared goal of being the best and the fastest. Every role and member are as important as any other within the team. With a growing number of actors involved along the life cycle of RAS, there is a need to ensure that all parties work toward a common goal that stands above the interests of particular stakeholder affiliations and is integrated under one team's effort. The F1 mindset should include the political authorities, whose support and will are essential to the effectiveness of missions that deploy RAS.

5.4. Managing private partnerships (PPP) and market competition

One of the challenges of the military contractor is to balance the cooperation with reliable and trustworthy partners and the management of supply from new innovative competitors. Long-lasting arrangements may result in high dependency on a single provider, who may use his pivotal position to "increase charges and lower quality" while minimizing the possibility of effective oversight.[30] Balancing the risks and benefits associated with both market competition and close PPP is needed to achieve 'the best of both worlds' during the entire life cycle of RAS. One of the ways in which this situation is being addressed in the United States is through open bidding acquisition processes, accompanied by an additional process of scouting revolutionary and

[29] Clarke, "The Arrow Missile: The United States, Israel and Strategic Cooperation," 483 ("Israel has employed US weaponry contrary to US law and policy, incorporated US technology into Israeli weapons systems without prior approval, and made improper transfers of US missile and other defense systems and technologies to other countries, including Chile, China, and South Africa.").

[30] Perlo-Freeman and Sköns, "The Private Military Services Industry," 15.

emerging tech companies in order to increase the number of providers.[31] At the same time, due to the complexity and risks related to the development of RAS, it is often a preferred option to work with trusted partners, whose long-standing performance and relationship provides a sense of confidence.

6. Recommendations

This study reveals that in order to achieve an effective cooperation along the life cycle of RAS long-lasting relationships are required, such that are supported by clearly defined common goals, harmonized procedures, and shared understanding. This study highlights organizational, legal, and practical solutions to improve the effectiveness of cooperation with RAS. It is apparent that the dependency of RAS functionalities on the initial design is critical, thus highlighting the need to integrate and manage the cooperation in an iterative process that includes all parties, from the front developers to the end-users.

Based on the above-outlined considerations, the following recommendations are made to the armed forces in order to improve cooperation with a range of different stakeholders regarding RAS.

Development

1. *Establish* close communication from the early design phase onwards between diverse stakeholders (i.e. military customers and users, engineers, academics, civil society representatives, legal/ethical experts, and policy-makers) in order to improve implementation of interdisciplinary considerations into the functional and technical parameters of RAS.

2. *Ensure* that the contracting arrangement with external parties includes a clear division of tasks and responsibilities from the early design phase. The military should carefully consider how to establish a long-term, trusted relationships with the RAS developer/producer that will extend into other stages of the RAS life cycle on the one hand, whilst maintaining the ability to change partnership in case of ill-performance on the other.

3. *Create* incentives for new parties to enter the military RAS scene while fostering trust amongst current partners. This could take the form of offering fellowships to academic researchers and private entities to continue innovating RAS of autonomous systems, the organization of national competitions promoting participation of researchers and engineers, or offering financial incentives (such as tax reliefs or state funds) to private companies to encourage cooperation with the public sector in the creation of RAS.

[31] Allen and Chan, "Artificial Intelligence and National Security," 14 (An example is IN-Q-TEL company that searches for additional companies to participate in the governmental contracts.) .

Integration

4. *Develop* effective training programs in cooperation with RAS developers in order for personnel to gain an understanding of the system, to improve technical literacy, to build trust, and to adjust team dynamics.

5. *Test* RAS in an environment that is as close as possible to the intended operational environment in order to provide quality reassurance and improve users' trust in and understanding of the system (i.e. functions, limitations and possibilities).

6. *Accompany* the hand-over of the system with a clear division of future responsibilities, accountability for system failures, servicing, and software updates. This could be realized through the creation of licensing models in which the developer remains the owner and the party responsible for upgrades and quality checks.

7. *Incorporate* a wider community of internal stakeholders early in the process to assure that necessary organizational, procedural, and doctrinal changes that stretch beyond the scope of actual units in which RAS are introduced. For example, RAS may involve the hiring of different sorts of personnel, tactics and procedures that affect a wider operational deployment.

Use

8. *Outline* a clear division of responsibilities and control to help to reduce automation bias, promote compliance with international legal obligations and prevent 'mode confusion'.

9. *Conduct* post-operation evaluations to reflect upon ways in which the system aided the operation, as well as, failures to serve mission objectives. Considerations should be communicated with relevant stakeholders, including developers and designers of RAS, and personnel who interact with similar RAS in other operational environments.

10. *Further integrate* third party private actors into the re-configuration and upgrading of system functions after deployment.

11. *Provide* military personnel and relevant partners with adequate cyber awareness trainings specific to the additional risks associated with the use of RAS.

12. *Consider* an incentive-based scheme, in which higher safety measures and risk aversion are rewarded to mitigate unintended risks.

Life cycle management

13. *Agree* upon a clear division of tasks, investments and responsibilities between stakeholders that among others include, hand-over arrangements, quality control, liability, servicing, maintenance, and software updates.

14. *Exercise* meaningful oversight over all stakeholders, including private contractors, in order to ensure the implementation of relevant legal and ethical restrictions. This may take the form of internal guidelines or codes of conduct, supported by strong communication mechanisms.

15. *Prevent* proliferation of RAS elements by partners beyond the established cooperation through auditing and enforcement of contracting responsibilities.

16. *Promote* a 'Formula 1 mindset' between developers, technicians, politicians, and end-users of RAS whereby a common sense of urgency is shared by a diverse team that orients itself toward a clearly defined goal.

Bibliography

Allen, Greg, and Taniel Chan. "Artificial Intelligence and National Security." Belfer Center for Science and International Affairs, July 2017. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

"Army Cyber Training and Education within Finabel Member States." FINABEL European Army Interoperability Center, 2019. http://finabel.org/wp-content/uploads/2019/01/FQ_Cyber_Training_and_Education_Web2.pdf.

Bromley, Mark, and Giovanni Maletta. "The Challenge of Software and Technology Transfers to Non-Proliferation Efforts," n.d.

Chavannes, Esther, and Amit Arkhipov-Goyal. "Towards Responsible Autonomy: The Ethics of Robotic and Autonomous Systems in a Military Context." The Hague: The Hague Centre for Strategic Studies, September 2019. https://www.hcss.nl/sites/default/files/files/reports/Towards%20Responsible%20Autonomy%20-%20The%20Ethics%20of%20RAS%20in%20a%20Military%20Context.pdf.

Chavannes, Esther, Klaudia Klonowska, and Tim Sweijs. "Governing Autonomous Weapon Systems." Den Haag: The Hague Centre for Strategic Studies, February 13, 2020.

Clarke, Duncan L. "The Arrow Missile: The United States, Israel and Strategic Cooperation." *Middle East Journal* 48, no. 3 (1994). https://www.jstor.org/stable/4328717.

Kortenkamp, David, and Reid Simmons. "Robotic Systems Architectures and Programming." In *Springer Handbook of Robotics*, edited by Bruno Siciliano and Oussama Khatib, 187–206. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. https://doi.org/10.1007/978-3-540-30301-5_9.

Perlo-Freeman, Sam, and Elisabeth Sköns. "The Private Military Services Industry." Stockholm International Peace Research Institute, September 2008. https://www.sipri.org/publications/2008/sipri-insights-peace-and-security/private-military-services-industry.

Platts, Jon, Mary Cummings, and Rory Kerr. "Applicability of STANAG 4586 to Future Unmanned Aerial Vehicles." In *AIAA Infotech@Aerospace 2007 Conference and Exhibit*. Rohnert Park, California: American Institute of Aeronautics and Astronautics, 2007. https://doi.org/10.2514/6.2007-2753.

"Robotic and Autonomous Systems of Systems Architecture." Army Science Board. The Army Science Board, Department of the Army, January 15, 2017. https://apps.dtic.mil/dtic/tr/fulltext/u2/1058366.pdf.

"Safety, Unintentional Risk and Accidents in the Weaponization of Increasingly Autonomous Technologies." The United Nations Institute for Disarmament Research, 2016. https://www.unidir.org/files/publications/pdfs/safety-unintentional-risk-and-accidents-en-668.pdf.

Slijper, Frank, Alice Beck, and Daan Kayser. "State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons." Pax for Peace, April 2019.

"The U.S. Army: Robotic and Autonomous Systems Strategy." U.S. Army Training and Doctrine Command, March 2017. https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf.

Verbruggen, Maaike. "The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems." *Global Policy* 10, no. 3 (September 2019): 338–42. https://doi.org/10.1111/1758-5899.12663.

Wasiak, Radek. "What Is the Incentive in Insurance Premiums?" European Agency for Safety and Health at Work, November 16, 2009.

https://osha.europa.eu/sites/default/files/seminars/documents/Radek%20Wasiak%20insurance%20premiums.pdf.