GENEVA ACADEMY
Académie de droit international humanitaire et de droits humains
Academy of International Humanitarian Law and Human Rights

WORKING PAPERS

The Future Digital Battlefield and Challenges for Humanitarian Protection: A Primer

HENNING LAHMANN
APRIL 2022

THE GENEVA ACADEMY A JOINT CENTER OF
GENEVA GRADUATE INSTITUTE
INSTITUT DE HAUTES ÉTUDES INTERNATIONALES ET DU DÉVELOPPEMENT
GRADUATE INSTITUTE OF INTERNATIONAL AND DEVELOPMENT STUDIES
UNIVERSITÉ DE GENÈVE
FACULTY OF LAW

TABLE OF CONTENTS

1. INTRODUCTION

Novel digital technologies are set to revolutionise the ways wars are fought. Recent situations of armed conflict, both between states and between states and non-state actors, have revealed glimpses into this future of warfare. Noteworthy examples are the sustained campaign of tactical drone strikes by Azerbaijan against Armenian forces,[1] the purported deployment of autonomous armed drones in Libya,[2] or the use of AI-supported intelligence, surveillance, and reconnaissance (ISR) technologies,[3] including with the support of drone swarms,[4] by the Israeli Defence Forces during its latest military campaign in Gaza.

The increased employment of algorithmic decision-making systems that utilise vast amounts of data generated with the help of significant advances in unmanned aerial vehicle (UAV), space,[5] and sensor technologies,[6] fused in real time with further digital data sources such as social media activity, online behaviour, and other "publicly available information"[7] as well as mobile communications data, have begun to create ecosystems of constant military surveillance.[8] The far-reaching legal and ethical implications of these developments for affected civilian populations are still in the early stages of being properly analysed and understood. At the same time, the use of cyber tools continues to make inroads among state actors, both as an element of military operations during armed conflict and as part of ongoing, low- to mid-intensity encounters between great powers during peacetime.[9] Here, too, much is left to be examined to properly assess the potential

[1] Crabtree J, 'Gaza and Nagorno-Karabakh Were Glimpses of the Future of Conflict' [2021] Foreign Policy ‹https://foreignpolicy.com/2021/06/21/gaza-nagorno-karabakh-future-conflict-drones/›; Gady F-S and Stronell A, 'What the Nagorno-Karabakh Conflict Revealed About Future Warfighting' (World Politics Review, 19 November 2020)‹https://www.worldpoliticsreview.com/articles/29229/what-the-nagorno-karabakh-conflict-revealed-about-future-warfighting›.

[2] Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council, UN Doc. S/2021/229, 8 March 2021, para. 63, https://undocs.org/S/2021/229.

[3] Dar Y, 'Israel Says It Fought World's First "Artificial Intelligence War" Against Hamas' The Eurasian Times (29 May 2021) ‹https://eurasiantimes.com/israel-sys-it-fought-worlds-first-artificial-intelligence-war-against-hamas/›; Ben-Yishai R, 'How Data and AI Drove the IDF Operation in Gaza' YNet News (29 May 2021) ‹https://www.ynetnews.com/magazine/article/SJ2rHS6Y00›.

[4] Gross JA, 'In Apparent World First, IDF Deployed Drone Swarms in Gaza Fighting' The Times of Israel (10 July 2021) ‹https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/›.

[5] Reed J, Routh A and Mariani J, 'Information at the Edge: A Space Architecture for a Future Battle Network' (Deloitte Insights, 16 November 2020) ‹https://www2.deloitte.com/us/en/insights/industry/public-sector/future-space-weapons-space-architecture.html›.

[6] The Economist, 'Open-Source Intelligence Challenges State Monopolies on Information' [2021] The Economist ‹https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information›: "[Sensors] may also show things which, wavelength-restricted as their own eyes are, human interpreters have yet to imagine. It is in part to guard against missing such things that satellite images are increasingly fed into machine-learning software which will see patterns humans might not pick out, or even think to look for."

[7] See Smagh NS, 'Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition' (Congressional Research Service 2020) R46389 ‹https://fas.org/sgp/crs/intel/R46389.pdf›, p. 16 and 31.

[8] Scoles S, 'It's Sentient: Meet the Classified Artificial Brain Being Developed by US Intelligence Programs' [2019] The Verge ‹https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai›; Schultz RH and Clarke RD, 'Big Data at War: Special Operations Forces, Project Maven, and Twenty-First Century Warfare' (Modern War Institute, 25 August 2020) ‹https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/›.

[9] Van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›; Stacey E, 'The Future of Cyber Warfare – An Interview with Greg Austin' (Strife, 26 April 2020) ‹https://www.strifeblog.org/2020/04/26/the-future-of-cyber-warfare-an-interview-with-greg-austin/›.

consequences for civil societies.[10] Complemented by important developments in robotics and perhaps at some point in the future even extending to cybernetically enhanced human soldiers,[11] the progressing digitisation of military technology is set to involve transformative shifts in the ways in which future conflicts will play out in inter-state constellations as well as in regard to conflicts between states and non-state armed groups. These novel digital technologies will inevitably shape how political and military decision-makers conceive the possibilities and constraints of contemporary warfare and thus impact policy in relation to future conflict.[12] This, in turn, implies that existing international legal frameworks will come under increasing pressure to be responsive to this momentous development, in particular with a view to future humanitarian protection needs.

To date, international legal scholarship has primarily addressed issues that encompass important but limited aspects of the digitisation of conflict, most prominently the law applicable to cyber operations[13] or the legal and ethical implications of the development and prospective use of lethal autonomous weapons systems (LAWS).[14] Without ignoring these more specific questions, the present framing paper attempts to zoom out and expand the scope of consideration. Taking a holistic perspective, its main focus are the convergent effects of the different technological trends in the areas of AI, cyber, space, robotics, drones, and sensor systems, asking what the "future digital battlefield" might entail for the protection of affected individuals and societies as provided by existing legal frameworks.

To this end, the paper first provides an overview of the various technologies that, taken together, constitute the "future digital battlefield", with a specific focus on those areas that have not received as much attention to date. On the basis of these partially speculative descriptions, the second part highlights a few legal subject areas that entail some of the potentially most consequential implications for future humanitarian protection in armed conflict. Rather than presenting fully formed answers to the questions posed by novel digital technologies in the military or an in-depth legal analysis of each identified challenge, the purpose of this primer is to provide an informed and critical outline of the most urgent issues concerning the possible ramification of an ever-more digitalised battlefield in order to frame the emerging debate among scholars and political decision-makers.

To that end, in addition to original research conducted by the author, the paper draws on the findings and discussions of an online expert workshop conducted on 12 August 2021.[15]

---

[10] International Committee of the Red Cross, 'The Potential Human Cost of Cyber Operations' (2019) ‹https://www.icrc.org/en/document/potential-human-cost-cyber-operations›; Geiß R and Lahmann H, 'Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf›.

[11] See Shereshevsky Y, 'Are All Soldiers Created Equal? – On the Equal Application of the Law to Enhanced Soldiers' (2021) 61 Virginia Journal of International Law 271.

[12] See Dorsey J and Amaral N, 'Military Drones in Europe: Ensuring Transparency and Accountability' (Chatham House 2021) ‹https://www.chathamhouse.org/sites/default/files/2021-04/2021-04-30-military-drones-europe-dorsey-amaral.pdf›, p. 7.

[13] See only Schmitt MN (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017); Moynihan H, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019) ‹https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf›; Delerue F, Cyber Operations and International Law (2020).

[14] See only Human Rights Watch, 'Losing Humanity. The Case against Killer Robots' (Human Rights Watch 2021) ‹https://www.hrw.org/sites/default/files/reports/arms1112*ForUpload.pdf*›; International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach' (2019) ‹https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach›.

[15] The workshop participants were Greg Austin, Anja Dahlmann, Kristen E. Eichensehr, Lindsay Freeman, Arthur Holland Michel, Asaf Lubin, Kubo Mačák, Rebecca Mignot-

2. ELEMENTS OF THE FUTURE DIGITAL BATTLEFIELD: TECHNOLOGY OVERVIEW

The following section describes some of the determining individual elements that jointly characterise the "future digital battlefield". To the extent that some of these technologies have previously been described in more detail elsewhere, they will only be addressed briefly. What is important to note at the outset is that whatever these technologies signify and imply in isolation, it is crucial to emphasise and analyse the convergent effects of the employment of these different technologies, and what these effects imply for the continuing ability of existing legal frameworks to regulate or mitigate possible adverse consequences for humanitarian protection.

2.1 OFFENSIVE CYBER CAPABILITIES

There is broad consensus today that the digital transformation of society of over the past three decades has also ushered in a new era of conflict with entirely new methods to carry out military operations. Most recently, the dawn of the age of cyber warfare has perhaps been the most obvious and widely discussed aspect of this paradigm shift. The author has addressed the issue of the use of cyber means in the military in more detail elsewhere,[16] but as an integral component of the emergent digitalisation of the battlefield, it merits brief mention here. The ways in which offensive cyber capabilities could support future military operations are manifold. While the employment of such tools might at times aim at complementing kinetic resources, a potentially more momentous shift, both from a perspective of military strategy and from the humanitarian protection angle, is the significant expansion of possibilities to directly impact adversarial states without any use of kinetic force at all.

During the course of more traditional military operations, cyber capabilities might be leveraged for destructive or disruptive effects as part of what has recently been dubbed "all-domain manoeuvre warfare",[17] i.e. the creation of "decision advantage enhanced through (...) cyberspace to enable operations in the Ground, Air, and Maritime Domains to deter and defeat" an adversary.[18] This might include the manipulation or disabling of the opponent's weapons systems by way of inserting malware,[19] digitally attacking adversarial ISR systems or stored intelligence data in order to thwart reconnaissance activities, or more generally disrupting the adversary's digital infrastructures, as first on view in the armed conflict between Russia and Georgia in 2008.[20] One real-world example to mention in this context are the extensive cyber operations by the U.S. and its allies in the fight against ISIS, not only digitally attacking the terrorist group's

Mahdavi, Nema Milaninia, Khadidja Nemar, Giacomo Persi Paoli, Sasha Radin, Chiara Redaelli, Yahli Shereshevsky, Talita de Souza Dias, and Noëlle van der Waag-Cowling.

[16] See Geiß R and Lahmann H, 'Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf›; Geiß R and Lahmann H, 'Protection of Data in Armed Conflict' (2021) 97 International Law Studies 556.

[17] See Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

[18] See ‹www.jcs.mil/Portals/36/Documents/Doctrine/MECC2019/mecc2019day1brief6*jointfutures*concepts.pdf?ver=2019-10-17-143319-517›.

[19] See Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

[20] See Lawson E, 'Into the Ether: Considering the Impact of the Electromagnetic Environment and Cyberspace on the Operating Environment' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*operating*enviroment*web.pdf*›, 56.

communication networks and devices that were used for propaganda campaigns and recruiting efforts[21] but even disrupting active drone operations by the organisation.[22]

Perhaps even more far-reaching is the prospect of employing offensive cyber capabilities to replace traditional military operations that rely on some sort of kinetic force. Some of such operations might be launched with the intention to minimise risks of large-scale damage at the targeted adversarial objects and thus to decrease escalation risks. Operation Olympic Games, better known as the Stuxnet malware, deployed by the U.S. and Israel to sabotage Iranian uranium enrichment facilities in Natanz, may serve as an example for a cyber operation that, while intentionally causing physical damage, was arguably less destructive than had the militaries and intelligence agencies of the two states attempted to achieve the same effects with kinetic weapons launched from fighter jets or drones.[23] At the same time, over the past decade we have seen instances of disruptive military cyber operations targeting critical infrastructures in other states, such as the electrical grid,[24] or against civilian assets that had serious, probably unintended effects in a large number of countries.[25] Such cases have been on the rise, perhaps even slowly starting to supersede the targeting of more traditional military objects,[26] leading to the observation that the conduct of conflict is slowly shifting towards the coercion and control of civilian populations in adversarial states instead of attempting to defeat the opposing military forces.[27] Recent assessments have pointed out the many risks for civilian persons and objects resulting from such operations.[28] In light of current capacities and strategies, it has been suggested that when it comes to the use of offensive military cyber technologies in conflict situations, the overall picture resembles that of air warfare in 1914 – which implies that more large-scale, increasingly sophisticated operations with more destructive effects are to be expected in the coming one to two decades.[29]

2.2 INFORMATION WARFARE

Propaganda and other efforts to obtain informational advantage over the opponent have always been part and parcel of military operations in and beyond armed conflict.

21 See Work J, 'The American Way of Cyber Warfare and the Case of ISIS' (Atlantic Council, 17 September 2019) ‹https://www.atlanticcouncil.org/blogs/new-atlanticist/the-american-way-of-cyber-warfare-and-the-case-of-isis/›; Temple-Raston D, 'How the U.S. Hacked ISIS' (NPR, 26 September 2019) ‹https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis›; Bronk C and Anderson GS, 'Encounter Battle: Engaging ISIL in Cyberspace' (2017) 2 The Cyber Defense Review 93.

22 Warrell H, 'UK Targeted ISIS Drones and Online Servers in Cyber Attack' Financial Times (7 February 2021) ‹https://www.ft.com/content/360a8e1c-b241-40f7-b944-45a4f8854ac5›.

23 See Zetter K, 'NATO Researchers: Stuxnet Attack on Iran Was Illegal "Act of Force"' (Wired, 25 March 2013) ‹http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/›.

24 See Park D and Walstrom M, 'Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks' (The Henry M. Jackson School of International Studies, 11 October 2017) ‹https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/›.

25 See Greenberg A, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' [2018] Wired ‹https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/›.

26 Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021), 34.

27 van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›.

28 See Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021); van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›.

29 Expert assessment during workshop

However, the internet and other networked digital technologies have vastly expanded the possibilities to manipulate the information ecosystem to the detriment of the opponent, with a wide range of potential ramifications for humanitarian protection, as already explored in detail in a previous paper.[30] Leveraging social media and other channels of digital communication, militaries are now able to carry out complex information operations to deceive, influence, or coerce members of adversarial armed forces. More importantly, in a similar way as certain cyber capabilities have started to be used, the spread of false and otherwise misleading information may be employed to directly impact the civilian population in another country for strategic gain, achieving political outcomes that hitherto required the unleashing of kinetic force. This is not at all necessarily deescalatory: In certain circumstances, the deployment of such tools can result in heightened tension or even intra-communal violence among the target population.[31]

2.3 ARTIFICIAL INTELLIGENCE

The most fundamental shifts in military activities on both the strategic and operational level as part of the larger "future digital battlefield" are expected to be enabled by the continuing progress of technologies that utilise machine-learning algorithms (ML) and other forms of what is commonly described as artificial intelligence (AI). While there is no generally recognised definition of AI,[32] in its most general sense AI can be understood as "a 'constellation' of processes and technologies enabling computers to complement or replace specific tasks otherwise performed by humans, such as making decisions or solving problems".[33] One distinction often made in this context is between "general AI", a supposedly highly intelligent form of processing capable of fulfilling a great number of different tasks that approaches human-level cognitive abilities – a technology that does not yet, and indeed might well never, exist – and "narrow artificial intelligence", which refers to computer systems that are able to "perform programmed tasks (human-developed algorithms) in specific domains".[34] As a sub-category of narrow AI, "machine learning" describes the currently prevalent method of training algorithms. Systems relying on this technology are trained on vast amounts of data that allow them to build their own models to effect certain outcomes – i.e. to make predictions – instead of operating on the processing of pre-programmed rules, as the previous AI paradigm had envisioned. This means that the output depends on a number of variant and interdependent factors, such as the type of learning process and the resulting model, which is a function of the data with which the algorithm is fed. On of the inherent features of this approach is that a human operator has only limited insight into the exact mechanism of learning, which makes the outcome of the operation unpredictable at least to some degree, depending on the circumstances of a given situation and environment.[35]

As an all-purpose technology not unlike

[30] Geiß R and Lahmann H, 'Protecting the Global Information Space in Times of Armed Conflict' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf›.

[31] International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2019), 28-29.

[32] Lewis DA, 'Legal Reviews of Weapons, Means and Methods of Warfare Involving Artificial Intelligence: 16 Elements to Consider' (ICRC Humanitarian Law & Policy, 21 March 2019) ‹https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/›.

[33] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/73/348 (29 August 2018), p. 3.

[34] Id., 4.

[35] International Committee of the Red Cross, 'Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control' (2019), p. 14-15.

electricity or network communications, it makes little sense to approach AI as one uniform development that is responsive to one-size-fits-all regulatory or policy approaches. Therefore, the following sections attempt to outline the "AI revolution" in the military by highlighting some of the individual subject areas where the technology promises to prove the most momentous and far-reaching in light of humanitarian concerns. This means that uses of AI that will become of increasing significance for the internal organisation of armed forces, such as employing ML algorithms to optimise maintenance cycles for military equipment, are not addressed. Furthermore, it is important to note that not all of the subsections are, strictly speaking, analytically separate. Autonomous unmanned aerial vehicles (UAVs) (2.3.2) may have the capability to be employed as lethal autonomous weapons systems (LAWS) (2.3.1) or be used for intelligence, surveillance, and reconnaissance (ISR) tasks (2.3.3) or targeting (2.3.4). Battlefield command & control as well as AI-supported targeting will depend on ISR and may utilise autonomous cyber tools (2.3.5), and so on.

2.3.1 LETHAL AUTONOMOUS WEAPONS SYSTEMS

The proliferation of AI systems in the military has to date been most elaborately discussed in the context of the development and possible deployment of so-called lethal autonomous weapons systems. According to the International Committee of the Red Cross, a LAWS is a system "that has autonomy in its 'critical functions', meaning a weapon that can select (i.e. search for or detect, identify, track) and attack (i.e. intercept, use force against, neutralise, damage or destroy) targets without human intervention".[36] While quite a few states are developing such autonomous weapons or have at least expressed the intent to do so in the future,[37] to date, real-world cases of the actual deployment of such systems remain few and far between. In March 2021, a report by the Panel of Experts on Libya addressed to the UN Security Council drew considerable attention by pointing to the purported use of the Turkish-built autonomous lethal drones "STM Kargu-2" in a combat situation between warring factions of the Libyan civil war. According to the report, the unmanned aerial vehicle had been "programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget and find' capability".[38] At the same time, other experts cast doubt on the significance of the finding, cautioning that the report had in fact not made clear whether the drone had acted in a truly autonomous fashion when engaging its target.[39]

Generally speaking, observers have pointed out that in the context of LAWS, "autonomy" will remain a relative concept no matter the actual AI capabilities of the system. As noted by Paul Scharre, no weapon "will be 'fully autonomous' in the sense of being able to perform all possible military tasks on its own. Even a system operating in a communications-denied environment will still be bounded in terms of what it is allowed to do. Humans will

[36] International Committee of the Red Cross, 'Autonomous Weapon Systems: Is It Morally Acceptable for a Machine to Make Life and Death Decisions?' (ICRC, 13 April 2015) ‹https://www.icrc.org/en/document/lethal-autonomous-weapons-systems-LAWS›.

[37] In a recent report, Human Rights Watch listed China, Israel, Russia, South Korea, the United Kingdom, and the United States as investing "heavily" in the development, and Australia, Turkey, as well as other countries as "making investments", see Wareham M, 'Stopping Killer Robots. Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control' (Human Rights Watch 2020) ‹https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and#›.

[38] UN Security Council, 'Letter Dated 8 March 2021 from the Panel of Experts on Libya Established Pursuant to Resolution 1973 (2011) Addressed to the President of the Security Council' (UN Security Council 2021) S/2021/229 ‹https://undocs.org/S/2021/229›, para. 63.

[39] See Cramer M, 'A.I. Drone May Have Acted on Its Own in Attacking Fighters, U.N. Says' The New York Times (3 June 2021) ‹https://www.nytimes.com/2021/06/03/world/africa/libya-drone.html›.

still set the parameters for operation and will deploy military systems, choosing the mission they are to perform."[40] Despite this reservation, the subject of LAWS and in particular the question how much "meaningful human control" must be retained for such a system to be ethically and legally justifiable remains one of the most hotly debated issues in the context of the use of AI in military applications and the future digital battlefield more generally, both in academic environments and among states. Since 2017, with a mandate from the Certain Conventional Weapons Meeting of High Contracting Parties, a Group of Governmental Experts (GGE) has been attempting to grapple with "questions related to emerging technologies in the area of lethal autonomous weapons systems". In 2019, the GGE published "11 Guiding Principles on LAWS".[41]

2.3.2 UNMANNED AERIAL VEHICLES AND DRONE SWARMS

While the public debate on AI in the military has been focusing on the issue of LAWS, the technology might be more useful in the short to mid term – and indeed become ubiquitous soon – in regard to applications that have nothing to do with autonomously engaging targets. One of the most important subject areas in this context is the employment of machine-learning algorithms in unmanned aerial vehicles, where it can be used for a variety of tasks such as autonomous navigation or surveillance activities that require only minimum human intervention.[42] Generally speaking, drones have become more and more important for military strategy over the past decade, not only as a preferred tool to conduct the "war on terror" but also more recently in the international armed conflict between Azerbaijan and Armenia.[43]

Potentially even more momentous is the development of robotic swarms that may consist of a large number of UAVs or other (e.g. land- or sea-based) systems.[44] Although not yet operational, the technology is set to add a further unprecedented layer of complexity to the future conduct of armed conflict. At its most basic conception, swarms may be defined as "multi-robot systems within which robots coordinate their actions to work collectively towards the execution of a goal".[45] Crucially, swarming properly understood implies that the entity taken as a whole is more than the sum of its parts; not only would the individual robots that make up the swarm not be capable of fulfilling the assigned tasks on their own, some complex effects of operating swarms would be inconceivable without the intricate – and to some degree unforeseeable – dynamics that emerge when the individual robots coordinate with each other autonomously, trying to find the

[40] Scharre P, 'Between a Roomba and a Terminator: What Is Autonomy?' (War on the Rocks, 18 February 2015) ‹https://warontherocks.com/2015/02/between-a-roomba-and-a-terminator-what-is-autonomy/›.

[41] See United Nations Office for Disarmament Affairs, Background on LAWS in the CCW, ‹https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/›.

[42] See Dorsey J and Amaral N, 'Military Drones in Europe: Ensuring Transparency and Accountability' (Chatham House 2021) ‹https://www.chathamhouse.org/sites/default/files/2021-04/2021-04-30-military-drones-europe-dorsey-amaral.pdf›, p. 15-16.

[43] See Crabtree J, 'Gaza and Nagorno-Karabakh Were Glimpses of the Future of Conflict' [2021] Foreign Policy ‹https://foreignpolicy.com/2021/06/21/gaza-nagorno-karabakh-future-conflict-drones/›; Gady F-S and Stronell A, 'What the Nagorno-Karabakh Conflict Revealed About Future Warfighting' (World Politics Review, 19 November 2020) ‹https://www.worldpoliticsreview.com/articles/29229/what-the-nagorno-karabakh-conflict-revealed-about-future-warfighting›.

[44] See e.g. Royal Marines, 'Drone Swarms Support Commando Forces Trials in a First for the UK's Armed Forces' (Royal Navy, 17 July 2021) ‹https://www.royalnavy.mod.uk/news-and-latest-activity/news/2021/july/17/210715-autonomous-advance-force-4›.

[45] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 24.

most efficient way to complete a mission by sharing resources and flexibly dividing tasks. This "swarm intelligence" may allow for increased coordination and speed in conflict situations.[46] The possible uses of swarms for the military are manifold and include "intelligence, surveillance and reconnaissance operations; perimeter surveillance and protection; distributed attacks; overwhelming enemy air defences; force protection; deception; search and rescue operations; countering swarms; and dull, dirty and dangerous tasks".[47]

Swarms pose intriguing questions about the feasibility and modelling of human control. While every single unit within a swarm acts autonomously, i.e. according to its own algorithmic setup, the swarm is itself an autonomous entity, encompassing the totality of the decentralised, autonomous decisions of each robotic entity. Therefore, human operators can only meaningfully exercise control over the entire swarm but not its constituent parts. In light its inherent complexity that may result in so-called "emergent behaviours" – i.e. behaviour that only occurs after the testing phase during actual missions – however, some experts have raised doubts as to the predictability and thus controllability of robotic swarming behaviour.[48] Others have argued that appropriate "design and modelling approaches" might nonetheless be capable of enabling proper human control.[49]

Aside from the issue of the possibility of human control, the very architecture of decentralised, autonomous robotic swarms requires a highly reliable communications infrastructure in order to enable both coordination between the individual autonomous entities and human command and control. This necessarily means that swarms are inherently vulnerable to outside interference by means of "jamming, spoofing, hacking, hijacking, manipulation or other electronic warfare attacks".[50] From a legal perspective, this implies an increased responsibility for armed forces employing drone swarms to secure such systems and ensure the ability to intervene in case a swarm starts behaving erratically and potentially dangerously for protected persons and objects, which will be addressed in more detail in Part 3 below.

As mentioned, despite some announcements to the contrary,[51] swarming technology properly understood has not yet been realised. While there have been reports that during its military campaign in Gaza in May 2021, the Israel Defence Forces became the first military to deploy drone swarms for purposes of ISR in a combat scenario,[52] it is questionable whether the large groups of small UAVs were in fact displaying true swarming capabilities by autonomously communicating and coordinating with each other.[53]

---

[46] Scharre P, 'Unleash the Swarm: The Future of Warfare' (War on the Rocks, 4 March 2015) ‹https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/›.

[47] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p.1.

[48] See Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021), p. 19.

[49] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 55.

[50] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 54.

[51] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 54.

[52] See Makewar A, 'Israel Used First-Ever AI-Guided Combat Drone Swarm in Gaza Attacks' (6 July 2021) ‹https://www.inceptivemind.com/israel-used-first-ever-ai-guided-combat-drone-swarm-gaza-attacks/19940/›; Dunhill J, 'First "AI War": Israel Used World's First AI-Guided Swarm Of Combat Drones In Gaza Attacks' IFL Science (2 July 2021) ‹https://www.iflscience.com/technology/first-ai-war-israel-used-worlds-first-aiguided-swarm-of-combat-drones-in-gaza-attacks/›.

[53] See Gross JA, 'In Apparent World First, IDF Deployed Drone Swarms in Gaza Fighting' The Times of Israel (10 July 2021) ‹https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/›; Dunhill J, 'First "AI War": Israel Used World's First AI-Guided

2.3.3 INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) AND FUSION ARCHITECTURES

When military decision-makers contemplate on the omnibus concept of the "future digital battlefield", a cornerstone of any evolving strategy is the large-scale use of AI for purposes of intelligence, surveillance, and reconnaissance activities, an area that is particularly suitable to take advantage of the capabilities of machine-learning technologies. Since the onset of the global "war on terror" prompted the sweeping expansion of intelligence activities on information and telecommunications network infrastructures to carry out wide-reaching and constant surveillance that became the defining feature of transnational counterterrorism,[54] the amount of data recording the behaviour of individuals gathered by states' security apparatuses has grown exponentially, with the result that no human can realistically take stock of, let alone analyse, the available information.[55] Today, the vast amounts of data obtained from citizens' online communication or social media activities[56] is complemented by and combined with visual or audiovisual feeds gained from a variety of sensors installed on satellites in geostationary or low Earth orbit[57] or UAV platforms that autonomously operate in conflict zones or elsewhere, able to cover a wide span of territory,[58] as well as the rapidly growing number of internet-of-things (IoT) devices that effectively act as remote sensors. As an expert recently noted succinctly, "pretty much everything is going to be connected; all things are potential sources of information".[59] To provide one example, through drone surveillance activities conducted as part of its global counterterrorism operations, in 2017 alone, U.S. Central Command reportedly collected 700,000 hours, or 80 years, of full-motion video material.[60] Naturally, to meaningfully examine such amounts of raw data is beyond any human analyst's capabilities;[61] only AI systems using machine-learning algorithms can feasibly parse through such massive troves of big data and look for conspicuous behavioural patterns or trends that may support more efficient and faster decision-making in conflict settings, both on an operational and a strategic level, and increase situational awareness on the battlefield.[62]

Swarm Of Combat Drones In Gaza Attacks' IFL Science (2 July 2021) ‹https://www.iflscience.com/technology/first-ai-war-israel-used-worlds-first-aiguided-swarm-of-combat-drones-in-gaza-attacks/›.

[54] Margulies J, '9/11 Forever' [2021] The Boston Review ‹https://bostonreview.net/war-security/joseph-margulies-911-forever›; Bhuta N and Mignot-Mahdavi R, 'Dangerous Proportions: Means and Ends in Non-Finite War' (2021) Asser Research Paper 2021-01, p. 22.

[55] See Frisk A, 'What Is Project Maven? The Pentagon AI Project Google Employees Want out Of' (Global News, 5 April 2018) ‹https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/›.

[56] Smagh NS, 'Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition' (Congressional Research Service 2020) R46389 ‹https://fas.org/sgp/crs/intel/R46389.pdf›, p. 16.

[57] Stacey E, 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady' (Strife, 9 September 2020) ‹https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/›.

[58] Schultz RH and Clarke RD, 'Big Data at War: Special Operations Forces, Project Maven, and Twenty-First Century Warfare' (Modern War Institute, 25 August 2020) ‹https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/›.

[59] Bayley J, 'Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist, NATO' (Defence IQ, 30 July 2018) ‹https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data›.

[60] Schultz RH and Clarke RD, 'Big Data at War: Special Operations Forces, Project Maven, and Twenty-First Century Warfare' (Modern War Institute, 25 August 2020) ‹https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/›.

[61] Id.

[62] See Konaev M, 'With AI, We'll See Faster Fights, But Longer Wars' (War on the Rocks, 29 October 2019) ‹https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/›; Bayley J, 'Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist, NATO' (Defence IQ, 30 July 2018)

The cutting edge of these advanced AI-supported ISR systems are so-called platform-independent fusion architectures that harvest data gathered by means of the latest high-fidelity sensor technologies across various platforms (air, space, ground assets) and numerous further sources (including social media activity, phone records, public administrative data about individuals or groups, and other publicly available open-source intelligence (OSINT) datasets), amalgamating vast swathes of unstructured data.[63] Experts expect this new generation of ISR to revolutionise military command and control, enabling the implementation of "battlefield management systems" that provide military commanders with an autonomously and dynamically analysed and prioritised, comprehensive operating picture in the field, with the potential to be accessible to all deployed personnel and thus to make decision-making during military operations both faster and more reliable. Ongoing projects that attempt to build large-scale systems capable of integrating these different types of data streams and providing real-time AI-based analysis include "Project Maven" (aka "Algorithmic Warfare Cross-Function Team"), launched in 2017,[64] which was recently incorporated into the "Advanced Battle Management System (ABMS)" of the U.S. Air Force as part of the development of a comprehensive "Joint All Domain Command and Control (JADC2)".[65] It is conceived as a "network-of-networks that aims to link 'every sensor to every shooter' across air, land, sea, space and cyber".[66] According to recent reports, the EU has started to consider funding the development of such technologies as well.[67] While more advanced fusion architectures are still in the planning stage,[68] at least "Project Maven" has reportedly already supported U.S. counterterrorism missions in the Middle East.[69] So far, the system is limited to the ability to assist human operators to process the large quantities of incoming data, lacking the sophistication to provide autonomously generated deductions that adequately take account of the broader context.[70] Another long-term U.S.-launched endeavour in this area is "Sentient",[71] an "artificial brain" mainly utilising geospatial data gathered from satellites and other sources to detect pattern anomalies that can predict "model

---

‹https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data›; Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

[63] Holland Michel A, 'There Are Spying Eyes Everywhere – And Now They Share a Brain' [2021] Wired ‹https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/›.

[64] Frisk A, 'What Is Project Maven? The Pentagon AI Project Google Employees Want out Of' (Global News, 5 April 2018) ‹https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/›.

[65] Barnett J, 'Latest ABMS Tests Break New Barriers on AI and Edge Cloud Capabilities' (FedScoop, 18 March 2021) ‹https://www.fedscoop.com/latest-abms-tests-ai-cloud-cybersecurity/›.

[66] Barnett J, 'Air Force Moving Project Maven into Advanced Battle Management System Portfolio' (FedScoop, 10 August 2020) ‹https://www.fedscoop.com/project-maven-air-forces-advanced-battle-management-system/›.

[67] Dorsey J and Amaral N, 'Military Drones in Europe: Ensuring Transparency and Accountability' (Chatham House 2021) ‹https://www.chathamhouse.org/sites/default/files/2021-04/2021-04-30-military-drones-europe-dorsey-amaral.pdf›, p. 15-16.

[68] Stacey E, 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady' (Strife, 9 September 2020) ‹https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/›.

[69] Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

[70] Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 9.*

[71] National Reconnaissance Office, 'NRO Key Talking Points: Sentient' (September 2016) ‹https://www.nro.gov/Portals/65/documents/foia/declass/ForAll/051719/F-2018-00108*C05112983.pdf*›.

adversaries' potential courses of action".[72] Despite the early stage of development of such architectures, experts predict that in the future, the fusion approach will lead to AI-enabled recommender systems technology that is able to "propose courses of action based on real-time analysis of the battlespace (as opposed to past behavior which in complex systems may not predict future behavior)".[73]

Reporting on the recent campaign launched by the Israel Defence Forces against Palestinian armed groups based in Gaza suggests that it may have been the first armed conflict in which one side directly benefited from the employment of AI-supported ISR that successfully fused data from different sources such as signals intelligence, visual intelligence, human intelligence, and geospatial intelligence in order to generate recommendations for targets such as rocket launchpads or groups of combatants in real time, and even to send out warnings of possible attacks against IDF units to tablets provided to commanders in the field.[74] However, it bears noting that this information has not been confirmed by sources independent of the IDF itself.[75] Either way, at least spokespeople for Israeli military went as far as calling the conflict the "first AI war".[76]

2.3.4 TARGETING

Naturally, the development of both LAWS and fusion architectures for ISR underlines the relevance that military decision-makers envision for AI system when it comes to the process of targeting during military operations. Having machine-learning algorithms take decisive steps as part of the "kill chain", i.e. that directly lead to engaging a military objective, goes beyond "mere" ISR, even if the latter might lead up to a targeting decision, while falling short of actually using force autonomously. This type of task can involve different algorithmic activities by the employed system, depending on the technology and the situation. It was recently reported that the latest iteration of the U.S. Air Force's ABMS is now capable of "directly aid[ing] in zeroing in on a target", which was considered a serious breakthrough.[77] Similarly noteworthy are accounts of the assassination of an Iranian nuclear scientist near Tehran in November 2020, in which Israeli intelligence apparently employed a facial recognition system to identify its target immediately prior to the strike, and a remotely controlled machine gun that used an AI system to compensate for the delay in satellite communication between weapon and human operator.[78] In both scenarios, it is obvious that

[72] Scoles S, 'It's Sentient: Meet the Classified Artificial Brain Being Developed by US Intelligence Programs' [2019] The Verge ‹https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai›.

[73] Konaev M, 'With AI, We'll See Faster Fights, But Longer Wars' (War on the Rocks, 29 October 2019) ‹https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/›.

[74] See Ahronheim A, 'Israel's Operation against Hamas Was the World's First AI War' The Jerusalem Post (27 May 2021) ‹https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371›; Ben-Yishai R, 'How Data and AI Drove the IDF Operation in Gaza' YNet News (29 May 2021) ‹https://www.ynetnews.com/magazine/article/SJ2rHS6Y00›; Dar Y, 'Israel Says It Fought World's First "Artificial Intelligence War" Against Hamas' The Eurasian Times (29 May 2021) ‹https://eurasiantimes.com/israel-sys-it-fought-worlds-first-artificial-intelligence-war-against-hamas/›; Kumon T, 'The First AI Conflict? Israel's Gaza Operation Gives Glimpse of Future' Nikkei Asia (28 June 2021) ‹https://asia.nikkei.com/Politics/International-relations/The-first-AI-conflict-Israel-s-Gaza-operation-gives-glimpse-of-future›.

[75] See Crabtree J, 'Gaza and Nagorno-Karabakh Were Glimpses of the Future of Conflict' [2021] Foreign Policy ‹https://foreignpolicy.com/2021/06/21/gaza-nagorno-karabakh-future-conflict-drones/›.

[76] Gross JA, 'IDF Intelligence Hails Tactical Win in Gaza, Can't Say How Long Calm Will Last' The Times of Israel (27 May 2021) ‹https://www.timesofisrael.com/idf-intel-hails-tactical-win-over-hamas-but-cant-say-how-long-calm-will-last/›.

[77] Barnett J, 'Latest ABMS Tests Break New Barriers on AI and Edge Cloud Capabilities' (FedScoop, 18 March 2021) ‹https://www.fedscoop.com/latest-abms-tests-ai-cloud-cybersecurity/›.

[78] See Bergman R and Fassihi F, 'The Scientist and the A.I.-Assisted, Remote-Control Killing Machine' The New York Times (18 September 2021)

even though the ultimate act of pulling the trigger, and thus to take the final decision to employ force, remains with a human – and a lot depends on the original mission design and the prior planning of the operation – the AI system was charged with carrying out a substantial proportion of the critical process.

2.3.5 CYBER WARFARE AND AI

The application of machine-learning algorithms and other types of AI to cyber operations has already begun, and it presents obvious advantages for military conduct in cyberspace.[79] For instance, the employment of machine learning greatly increases the chances of discovering vulnerabilities in code that the AI software could then exploit autonomously, which potentially leads to greater efficiency and speed of offensive cyber operations. To be sure, the same methods might be used to develop stronger defensive systems that are capable of automatically fending off malware or other adversarial intrusions into networks.[80] Furthermore, machine-learning algorithms can be very useful to scan and surveil the online activities of vast numbers of individuals[81] or to autonomously "prepare the digital battlefield" by planting malware in an adversary's networks that might be activated remotely in the case a conflict breaks out.[82] In this context, it is important to note that both the increased employment of machine-learning algorithms and the need to guarantee stable communication links between the different systems and components that constitute the "digital battlefield" greatly increases the attack surface, rendering the entire ecosystem much more susceptible to adversarial cyber conduct.[83] The implications of this will be addressed again in part 3.

2.3.6 INFORMATION WARFARE AND AI

Finally, the employment of artificial intelligence has already proven to greatly increase the potential impact of disinformation campaigns and other types of information warfare,[84] enabling any such efforts to become "more efficient, scalable, and widespread".[85]

‹https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html›.

[79] See Thornton R and Miron M, 'The Advent of the "Third Revolution in Military Affairs"; Is the UK Now Facing the Threat of AI-Enabled Cyber Warfare(?)' (Defence-In-Depth, 21 July 2020) ‹https://defenceindepth.co/2020/07/21/the-advent-of-the-third-revolution-in-military-affairs-is-the-uk-now-facing-the-threat-of-ai-enabled-cyber-warfare/›; van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›.

[80] See International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2019), p. 31.

[81] See Smagh NS, 'Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition' (Congressional Research Service 2020) R46389 ‹https://fas.org/sgp/crs/intel/R46389.pdf›, p. 16.

[82] See Buchanan B and Cunningham FS, 'Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis' (2020) 3 Texas National Security Review 54.

[83] See generally Herpig S, 'Securing Artificial Intelligence. Part 1: The Attack Surface of Machine Learning and Its Implications' (Stiftung Neue Verantwortung 2019) ‹https://www.stiftung-nv.de/sites/default/files/securing*artificial*intelligence.pdf›; Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 54; Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021), p. 7; Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021), p. 32.

[84] See International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2019), p. 31.

[85] Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 5-6.*

Possible use cases include the automatic generation of text that can easily be distributed digitally to disseminate false or misleading information,[86] the creation of deep-fake audiovisual content, the detection of rifts in a target population's social fabric to maximise a campaign's impact, the deployment of bots to artificially amplify subversive messaging directed at a target population, and to pursue automated agenda setting – in particular with more sophisticated bots that are programmed to credibly mimic real people's behaviour[87] – or the automatic calibration of micro-targeting methods in order to tailor content to receptive audiences. Machine-learning algorithms might automatically scrape social media to compile massive sets of users' personal behavioural data that can then be analysed to better understand local populations for the purpose of enabling algorithmic predictions as to the type of content that should be used for an operation.[88] Potentially even more far-reaching, according to reports, recent advances in natural language processing could even "leverage sentiment analysis to target specific ideological audiences".[89]

2.4 ROBOTICS AND SENSOR TECHNOLOGIES

The digital revolution of military activities could not fulfil its momentous potential without corresponding advances in robotics and sensor technologies. While sensors are required to produce much of the data that can then be analysed and exploited for further ends in the theatre of conflict, that is for the "digital" battlefield to emerge in the first place, many applications that utilise that data depend on complex robotic systems to execute the tasks that follow from data analysis. In the legal and policy literature, however, there is a general tendency to consider the implications of advanced robotics as a sub-category of the larger topic of autonomous weapons systems – even though the majority of robots will carry our tasks that are merely automated and do not require any degree of autonomy as properly understood.[90]

While the processing power behind sensors mounted on UAVs, planes, ships, submarines, satellites, or ground-based vehicles remains crucial to properly take advantage of the tons of data produced by current ISR architectures, recent progress in sensor technology itself plays an important part in the development of the "digital battlefield". Aside from more established sensors such as radar, sonar, video, infrared, and passive RF detection,[91] examples for the latest available technologies include infrared scan and track (IRST) sensors that work with super-cooled lenses "to search for and classify incredibly faint heat sources at long range"[92] or ground-based

[86] Villasenor J, 'How to Deal with AI-Enabled Disinformation' (Brookings, 23 November 2020) ‹https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/›.

[87] Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 5-6.*

[88] Jensen BM, Whyte C and Cuomo S, 'Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence' (2020) 22 International Studies Review 526, 532-33; Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 5-6.*

[89] Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 5-6.*

[90] See e.g. Winkler JD and others, 'Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense' (RAND Corporation 2019), p. 14-16.

[91] Zheng DE and Carter WA, 'Leveraging the Internet of Things for a More Efficient and Effective Military' (Center for Strategic & International Studies 2015) ‹https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy*files/files/publication/150915*Zheng*LeveragingInternet*WEB.pdf›, 14.

[92] Bronk J, 'Technological Trends' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*op*

multi-static passive radars that are able to detect "echoes in the background electromagnetic 'noise' of mobile-phone, television and radio transmissions (among others) to track aircraft without needing a primary radar emitter",[93] which might soon pose a problem to fighter jets using current stealth technologies. Other recent and noteworthy developments are lasers capable of identifying individuals over long distances by measuring their heartbeat or the remote utilisation of Bluetooth signals emitted by phones and other devices, or computer vision systems that can detect suspicious movements.[94]

To be sure, these developments in sensor technologies and the latest breakthroughs in artificial intelligence and machine learning as well as computers' increasing processing powers are directly interrelated. As pointed out by Bronk, "the extremely faint nature of the signals which are being tracked and huge number of false-positive readings and background clutter of one sort or another means that their practicality as operational tools is linked directly to the post-processing hardware and software available to refine the raw sensor data into a usable picture".[95] The technological progress of the different elements goes hand in hand and is deeply interdependent.

2.5 SPACE TECHNOLOGIES

A further essential aspect of the ongoing digitalisation of the battlefield is the increasing relevance of space assets as the backbone of the information and communications infrastructures that are needed to implement the conception of a constantly interconnected, responsive, and cross-domain "battle network architecture" which links members of the armed forces with sensors, data processing systems, and autonomously operating machines.[96] By itself, the utilisation of satellites for communication, ISR, missile warning, and positioning, navigation, and timing (PNT) is nothing new, having been around for decades.[97] Especially the U.S., China, and Russia have long-established infrastructures in space for these purposes.[98]

However, building a networked, digital combat infrastructure that relies on the continuous gathering, processing, and transmission of large amounts of data, for example for AI-supported command-and-control or remotely controlled means of warfare such as armed drones, puts new emphasis on the sophistication and complexity of space assets.[99] According to experts, a number of different types of military offensive cyber operations also depend on satellite-supported networks.[100] For this reason, several states have begun to develop and already deploy a new generation of space

*erating*enviroment*web.pdf*›, *p. 61-62.*

[93] Bronk J, 'Technological Trends' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*operating*enviroment*web.pdf*›, *p. 61-62.*

[94] Holland Michel A, 'There Are Spying Eyes Everywhere – And Now They Share a Brain' [2021] Wired ‹https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/›.

[95] Bronk J, 'Technological Trends' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*operating*enviroment*web.pdf*›, *62.*

[96] See Reed J, Routh A and Mariani J, 'Information at the Edge: A Space Architecture for a Future Battle Network' (Deloitte Insights, 16 November 2020) ‹https://www2.deloitte.com/us/en/insights/industry/public-sector/future-space-weapons-space-architecture.html›.

[97] Defense Intelligence Agency, 'Challenges to Security in Space' (2019) ‹https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space*Threat*V14*020119*sm.pdf›, p.8.

[98] See id.

[99] See International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2019), p. 32.

[100] Stacey E, 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady' (Strife, 9 September 2020) ‹https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/›.

technologies, among them smaller and more expendable low earth orbit satellites that can be launched into space at much lower cost and in much higher number, eventually forming networks of hundreds or even thousands of individual objects able to deliver internet from space, transmit new types of high-resolution earth imagery or even real-time video directly to members of the armed forces during ongoing missions, or support various AI applications in military systems.[101] On that account, it seems certain that the importance of space architectures will only grow as the digitalisation of the armed forces progresses further, becoming indispensable, from the perspective of military and political decision-makers, to the actual realisation of the potential of the "digital battlefield". In turn, this development has crucial implications for the required reliability and resilience of space assets both against kinetic attacks and adversarial cyber operations targeting orbiting platforms, communication links, or ground stations – especially in view of the fact that at least to date, few of these objects exclusively serve military purposes but are instead mostly of a dual-use nature, providing essential services for the functioning of civilian societies as well.[102]

2.6 HUMAN ENHANCEMENT TECHNOLOGIES

Further down the line, the all-encompassing digitalisation of the battlefield might not even spare human soldiers themselves. Among the variety of different concepts to apply the emergent field of "human enhancement technologies" to members of the armed forces is cybernetics. Broadly speaking, the technology comes down to the development of brain-machine interfaces (BCI) through brain implants or electrodes placed on the scalp or skull, ultimately enabling "seamless two-way interactions between soldiers and machines as well as between humans".[103] In the assessment of experts, such cybernetically enhanced individuals could remotely operate UAVs or weapons systems without the need to use joysticks or other instruments and with potentially increased situational awareness and oversight while reducing the complexities presented by current stationary user interfaces.[104] However, at this point, persistent questions regarding feasibility and long-term effects of such a technology, for example regarding the reversibility of the implantation of electrodes, render the introduction of BCI in the military unrealistic at least before the year 2030.[105] To some extent perhaps to be considered the logical endpoint of the "digital battlefield", there remains some reluctance not least in the population at large in light of the far-reaching ethical implications of such a technology.[106]

[101] Reed J, Routh A and Mariani J, 'Information at the Edge: A Space Architecture for a Future Battle Network' (Deloitte Insights, 16 November 2020) ‹https://www2.deloitte.com/us/en/insights/industry/public-sector/future-space-weapons-space-architecture.html›; Stacey E, 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady' (Strife, 9 September 2020) ‹https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/›.

[102] See International Committee of the Red Cross, 'The Potential Human Cost of the Use of Weapons in Outer Space and the Protection Afforded by International Humanitarian Law. Position Paper Submitted by the International Committee of the Red Cross to the Secretary-General of the United Nations on the Issues Outlined in General Assembly Resolution 75/36' (2021), p. 1-2.

[103] Shereshevsky Y, 'Are All Soldiers Created Equal? – On the Equal Application of the Law to Enhanced Soldiers' (2021) 61 Virginia Journal of International Law 271, 279.

[104] Emanuel P and others, 'Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD', p. 7.

[105] See Bronk J, 'Technological Trends' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*operating*enviroment*web.pdf*›, *p. 61.*

[106] Id., 9-10.

2.7 CONCLUSION: CONVERGENT EFFECTS

There can be no doubt that the described possibilities enabled by the digital revolution of military conduct will to a large extent determine future strategies in armed conflict, i.e. how and when states will deploy their armed forces, and to what ends. While much remains uncertain and will depend on concrete technological breakthroughs in the coming decade, a few overall trends may be predicted that result from convergent effects of the "future digital battlefield".

In the estimation of experts, first, one may observe two interdependent trends that are directly related to the increasing digitalisation: on the one hand, the development by states of anti-access and area-denial capabilities that aim at preventing an adversary from entering a physical or digital space; on the other, an opposing focus on creating opportunities in space and time to penetrate those areas physically or digitally by way of multi-domain operations that leverage the potentials of digital infrastructures. In such a scenario, time becomes a significant commodity, the efficient use of which can be facilitated by the widespread employment of novel digital technologies, in particular those that run with artificial intelligence. Machine-learning algorithms may help both with the quick analysis of incoming data streams from a multitude of sensors across the conflict zone and enable commanders to make faster decisions.[107] Whereas this leads to a compression of time, the same technologies allow for much greater remoteness – cyber operations launched against far-away adversaries; remotely controlled UAVs operating on different continents – leading to an expansion of space.

In turn, increased speed makes the further employment of AI further indispensable, up to the delegation of critical combat functions such as command-and-control or even decisions concerning the use of force against adversaries. Soon, such autonomous functionalities will become independent of any one specific platform, instead being distributed through complex system-of-systems architectures.[108] This development is not least directly correlated with the vastly increased amount of data that is produced by pervasive and constant, digitally enabled intelligence and surveillance activities, both online and, thanks to more sophisticated sensors, in the "physical" domain. As an expert remarked, "[w]e have to depend to some degree on AI and big data, analytic tools, machine learning as mechanisms to allow us to deal with that flood of data in the future and inform decision-making using those tools as part of the process". In other words, the increasing digitalisation of warfare begets the need for ever more digitalisation.[109] At some point, the only way to handle the enormous technological complexity of digitally interconnected military operations makes far-reaching reliance on and trust in the AI-supported assets virtually inevitable, whether decision-makers are actually comfortable with that development or not.[110]

Furthermore, the digital revolution of military conduct might lead to an increase in less lethal operations – for example by resorting to covert cyber operations that sabotage adversarial objects without the need to employ kinetic force,

[107] Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018*Final.pdf*›, *p. 9.*

[108] See Sauer F, 'Autonomy in Weapons Systems: Playing Catch up with Technology' (ICRC Humanitarian Law & Policy, 29 September 2021) ‹https://blogs.icrc.org/law-and-policy/2021/09/29/autonomous-weapons-systems-technology/›.

[109] Bayley J, 'Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist, NATO' (Defence IQ, 30 July 2018) ‹https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data›.

[110] Bronk J, 'Technological Trends' in Peter Roberts (ed), The Future Conflict Operating Environment Out to 2030 (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906*op*future*operating*enviroment*web.pdf*›, *p. 63.*

or by launching information operations that achieve military goals by coercing an enemy state – or, while using lethal force, at least to a better protection of civilians and civilian objects by the use of weapons that are more precise thanks to AI-supported ISR and command-and-control.[111] At the same time, these trends do not necessarily imply a reduction of potential harm caused by military conduct. As discussed elsewhere, these same technologies, while perhaps less lethal, provide states with entirely novel tools to exert pressure on adversaries, with potentially pervasive and persistent negative systemic effects on affected civilian populations.[112] This outlook has led one expert to predict "the predominance of persistent, low-intensity irregular conflict" in the future.[113] Instead of battles between armies, what we will see are wars "aimed at the control or coercion of large civilian populations, against whom the violence is now directed" by means of digital tools in cyberspace or the information ecosystem.[114]

3. IMPLICATIONS FOR HUMANITARIAN PROTECTION

As hinted at in the previous section, the continuing digital revolution of military affairs comes with great potential to make the conduct of armed conflict more efficient and powerful in the future. At the same time, the entirely novel modes of operation that digital technologies enable, especially with the widespread use of AI, have far-reaching and to date not completely understood implications for humanitarian protection, that is the safeguarding of the rights of protected persons and objects that may be affected by the conduct of warfare in the digital age. Some of the issues concern, for example, the normative reach of established rules of international law. Others cast doubt on the applicability of traditional legal regimes or relate to certain factual risks in connection with the large-scale deployment of digital technologies on the battlefield. The following sections present an outline of some of the most pressing subject areas from a legal perspective. The purpose of this framing exercise is to sketch out the larger questions posed by the "future legal battlefield", without necessarily presenting satisfying answers or providing detailed legal analysis. In total, five broad topics have been identified that merit closer scrutiny from the academic community as well as political and military decision-makers as the digital transformation of the armed forces advances in the coming decade: (1) legal thresholds and the application of

[111] This was claimed by the Israel Defence Forces in view of its widespread employment of AI-supported ISR in its military campaign in Gaza in May 2021, see Crabtree J, 'Gaza and Nagorno-Karabakh Were Glimpses of the Future of Conflict' [2021] Foreign Policy ‹https://foreignpolicy.com/2021/06/21/gaza-nagorno-karabakh-future-conflict-drones/›.

[112] See Geiß R and Lahmann H, 'Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf›; Geiß R and Lahmann H, 'Protecting the Global Information Space in Times of Armed Conflict' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf›.

[113] Van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›.

[114] Id.

existing humanitarian regimes; (2) the further entrenchment of the "military surveillance paradigm"; (3) the continuing dissolution of the spatial and temporal limits of the conflict zone; (4) states' positive obligations concerning the vulnerabilities of digital military technologies; and (5) questions pertaining human control, accountability, and responsibility. Each subject matter will be addressed in turn.

3.1 THRESHOLD QUESTIONS

The principal legal framework to provide humanitarian protection and to seek to limit the negative effects of warfare is the body of international humanitarian law (IHL), also known as the law of armed conflict (LOAC), consisting mainly of the four Geneva Conventions of 1949, the two Additional Protocols of 1977, and corresponding customary IHL. However, according to common Article 2 of the Geneva Conventions, the application of these rules is contingent on the existence of an armed conflict, which is generally considered to presuppose some degree of violence, understood as "the resort to armed force" according to a landmark ruling of the International Criminal Tribunal for the Former Yugoslavia.[115]

In situations where any of the novel digitally enhanced military equipment is deployed during the course of such an armed struggle between states, or even between a state and a non-state actor as part of a non-international armed conflict, there can thus be no doubt that such activity would be covered by the rules of IHL. However, the proliferation of the above described digital technologies greatly expands the military toolbox, providing means of conduct that might affect civilian populations or other protected persons and objects without reaching the stated threshold, thus rendering IHL inapplicable to such conduct. The assumption that the future of conflict will continue to become more and more "digital" suggests that the structural entanglement with the civilian sphere will only increase further. In this regard, two broad issue areas can be identified where this threshold issue will mainly play out.

First, as indicated above, the increasing resort to adversarial cyber operations and (dis)information activities demonstrates how the novel digital technologies facilitate "persistent, low-intensity irregular conflict"[116] that, rather than directly engaging an adversary's armed forces, mainly consists of a strategy of influencing or even coercing its civilian population. This increasing dissolution of the boundaries between the military and the civilian sphere is concerning insofar as conflicts are "fought" beyond the reach of the protective scope of IHL,[117] even though there can be no doubt that such conduct has potentially far-reaching ramifications for affected civilian societies and can indeed cause immense harm without the need to ever employ kinetic force at all.[118]

Second, considering the temporal dimension of the "digital battlefield", certain conduct in the context of the digitalisation of military affairs might be potentially harmful to legally protected persons and objects long before any type of "conflict" as properly understood even begins. For one, certain offensive cyber activities that amount to a "preparation of the battlefield", such

[115] ICTY, Tadić Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 70.

[116] van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (ICRC Humanitarian Law & Policy, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›.

[117] Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021), p. 34.

[118] See on this in more detail already Geiß R and Lahmann H, 'Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf›; Geiß R and Lahmann H, 'Protecting the Global Information Space in Times of Armed Conflict' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf›.

as the U.S. Cyber Command doctrines of "persistent engagement" and "defend forward",[119] are military operations that intentionally remain below the threshold of armed conflict.[120] But this does not mean that they do not have the potential to cause harm in civilian infrastructures, either by accident or on purpose, and to negatively affect the overall security and safety of infiltrated networks that might be necessary to control an electric grid, a water treatment facility, or other critical civil infrastructures. Furthermore, the pervasive and constant intelligence and surveillance activities made possible by digital technologies – be it on the internet or by means of satellites, UAVs, or closed-circuit television – affects targeted demographics without it being apparent what type of legal protection might be engaged at all.[121]

These considerations lead to the conclusion that a default resort to IHL in search for humanitarian protection against such military conduct might be conceptually misguided. Clearly, the matter needs to be framed more comprehensively and not simply through the traditional lens of the laws of armed conflict. However, the problem is that it is not always clear which legal framework is capable of stepping in. One obvious candidate, especially as far as AI-enabled ISR activities in "peacetime" are concerned, is of course international human rights law (IHRL). But despite ramped up efforts to apply a functional approach to the issue of the jurisdictional scope of human rights treaties,[122] to what extent rights such as privacy or general considerations concerning data protection are applicable extraterritorially when it comes to the activities of intelligence agencies remains an open question for the time being.[123] The recent decision by the Federal Constitutional Court of Germany to extend the reach of constitutionally guaranteed rights to privacy against the surveillance practices of the Federal Intelligence Service to non-German data subjects located outside of Germany[124] has widely been lauded as pointing in the right direction in this regard.[125] However, it remains to be seen whether this progressive approach will be taken more broadly and beyond the context of an individual state.

When it comes to adversarial military cyber and information activities below the threshold of armed conflict, international legal academia has become completely embroiled in extensive debates surrounding the application and substance of state-centred notions such as the principle or rule of sovereignty or the principle of non-intervention.[126] These ongoing discussions, which involve the increasingly active participation of state representatives publicly expressing official positions for example through the GGE and OEWG processes

[119] See Fischerkeller MP and Harknett RJ, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation' [2019] The Cyber Defense Review 267.

[120] Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021), p. 34.

[121] Whether IHL is at all concerned with issues of privacy and data protection will be addressed in the subsequent section.

[122] See with regard to the right to life UN Human Rights Committee, 'General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life' (2018) CCPR/C/GC/36.

[123] See for a progressive and far-reaching approach already Milanovic M, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81.

[124] 1 BvR 2835/17 (Federal Constitutional Court), judgment of 19 May 2020.

[125] See e.g. Çalı B, 'Has "Control over Rights Doctrine" for Extra-Territorial Jurisdiction Come of Age? Karlsruhe, Too, Has Spoken, Now It's Strasbourg's Turn' (EJIL: Talk!, 21 July 2020) ‹https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/›; Miller RA, 'The German Constitutional Court Nixes Foreign Surveillance' (Lawfare, 27 May 2020) ‹https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance›; Reinke B, 'Rights Reaching beyond Borders' (Verfassungsblog, 30 May 2020) ‹https://verfassungsblog.de/rights-reaching-beyond-borders/›.

[126] See only Moynihan H, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019) ‹https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf›.

at UN level, need not be reiterated here. Suffice it to add that at least regarding offensive yet low-intensity activities such as those under the "persistent engagement" umbrella, there is not yet any sense of emerging consensus whether these types of digital military activities meet any limits under international law at all.[127]

3.2 UTILISATION OF DATA AND THE EMERGENCE OF THE MILITARY SURVEILLANCE PARADIGM

By now it is not more than a truism to state that the digital transformation of society runs on data, meaning that none of the major shifts that the digitalisation of the economy, politics, and the ways in which people interact with each other in their daily lives would be conceivable without the constant collection and processing of vast amounts of data, whether of the personal or non-personal variety. Naturally, the same holds true for the "future digital battlefield"; both the conduct of military cyber operations and especially any application that employs machine-learning algorithms and other forms of AI is contingent on the availability of data and its real-time collection and analysis.[128] However, the implications of this development for the future of humanitarian protection are still not well understood. So far, scholarly debates have mainly revolved around the question of how to legally protect the availability and integrity of data against adversarial cyber operations, most prominently by zooming in on the issue whether data can be considered an "object" for the purpose of the rules of targeting in IHL.[129] The confidentiality of (personal) data, on the other hand, has so far by and large remained below the radar.[130]

What has been happening in military and security affairs over the past 20 years in relation to the utilisation and exploitation of personal data gathered through CCTV cameras in cities, by way of monitoring online behaviour, logging location and other sensitive data produced by smartphones and other networked devices, and more recently through footage shot by cameras mounted on drones in various contexts has run parallel to the emergence of what has famously been dubbed the "surveillance paradigm" of the digital economy.[131] As recently observed by a federal court in the U.S. in a case concerning Facebook's business practices, the social media company "monetizes its personal social networking monopoly principally by selling surveillance-based advertising. Facebook collects data on users both on its platform and across the internet and exploits this deep trove of data about users' activities, interests, and affiliations to sell behavioral advertisements".[132] In the security realm, the same principles began to take

[127] For a detailed discussion of the legal qualification of "persistent engagement" and "defend forward" and the status of the "rule of sovereignty" see Lahmann H, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' [forthcoming 2021] Duke Journal of Comparative & International Law.

[128] Husanjot Chahal, Ryan Fedasiuk and Carrick Flynn, Messier Than Oil: Assessing Data Advantage in Military AI, Center for Security and Emerging Technology, July 2020, https://cset.georgetown.edu/publication/messier-than-oil-assessing-data-advantage-in-military-ai/.

[129] See only Kubo Mačák, Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law (2015) 48 Israel Law Review 55.

[130] But see Robin Geiß and Henning Lahmann, Protection of Data in Armed Conflict (2021) 97 International Law Studies 556; Lubin A, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law' in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives (2021) ‹https://papers.ssrn.com/sol3/papers.cfm?abstract*id=3622061*›.

[131] Zuboff S, The Age of Surveillance Capitalism (2019); Zuboff S, 'Be the Friction - Our Response to the New Lords of the Ring' Frankfurter Allgemeine Zeitung (25 June 2013) ‹https://www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html›; Cavoukian A, 'Global Privacy and Security, by Design: Turning the "Privacy vs. Security" Paradigm on Its Head' (2017) 7 Health Technologies 329.

[132] Federal Trade Commission v Facebook, Inc [2021] Federal District Court for the District of Columbia 1:20-cv-03590-JEB, para. 3.

hold after the terrorist attacks of September 11, 2001, when political decision-makers concluded that the abstract and vague terrorist threat warranted the establishment of vast surveillance architectures that would utilise the wealth of private data generated by novel digital technologies,[133] a development that must be considered in the broader context of the turn towards automated profiling to make decisions about individuals.[134] In this regard, the most far-reaching shift in the last few years has been the development and increasing employment of fusion technologies as described above (see section 2.3.3). Whereas in the early stages of the ramped-up surveillance apparatus, individuals could still reasonably expect at least a degree of default privacy due to the fact that it remained difficult to correlate intelligence gathered through different digital sources, fusion technologies render it increasingly impossible to hide "in the spaces between each data point".[135]

It is crucial to note that from the technological perspective of machine-learning principles, the "surveillance paradigm" is an imperative. The way to train and test machine-learning algorithms is to feed them with large amounts of relevant data that the system uses to autonomously build statistical models to make predictions about future events. Although there have been efforts more recently to develop approaches to ML that do not depend on vast quantities of data, for example so-called "one shot" learning,[136] it has been pointed out that for the time being, "the only consistently and demonstrably reliable method to ensure that machine learning systems are validated against the widest possible degree of variance in data is to increase the size of the data sets on which they are trained and tested".[137] Using as much data as possibly available is the only way to "identify edge cases and develop fail-safe mechanisms to prevent catastrophic outcomes".[138] The insight that larger, and more diverse, datasets lead to better outcomes of algorithmic processes[139] is particularly relevant when looking at AI-supported military equipment used for ISR or targeting, including but not limited to in lethal autonomous weapons systems. Here, the data used both to train the algorithm and during actual missions are almost by default personal and directly relate to human beings, be it to pick out an individual with facial recognition software or to identify a suspicious "pattern of life" that may point to a terrorist who will then be targeted by an armed UAV.[140] The more such "pattern of life" analysis is handed over to machine-learning algorithms, the more the success of such operations is directly contingent on constant and pervasive multi-source surveillance of the population in the target area. In turn, the resulting "sensory overload" leads to a flood of data that can then only be handled by automating the process of analysis[141] – a mutually reinforcing cycle.

---

[133] See Evans JC, 'Hijacking Civil Liberties: The USA PATRIOT Act of 2001' (2002) 33 Loyola University Chicago Law Journal 933, 962 et seq.

[134] See Kaltheuner F and Bietti E, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2 Journal of Information Rights, Policy and Practice ‹http://doi.org/10.21039/irpandp.v2i2.45›, p. 5.

[135] Holland Michel A, 'There Are Spying Eyes Everywhere – And Now They Share a Brain' [2021] Wired ‹https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/›.

[136] See Flournoy MA, Haines A and Chefitz G, 'Building Trust through Testing' (2020) ‹https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf›, p. 9.

[137] Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021, p. 27.

[138] Flournoy MA, Haines A and Chefitz G, 'Building Trust through Testing' (2020) ‹https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf›, p.9.

[139] Taori R and others, 'Measuring Robustness to Natural Distribution Shifts in Image Classification', 34th Conference on Neural Information Processing Systems (2020) ‹https://proceedings.neurips.cc/paper/2020/file/d8330f857a17c53d217014ee776bfd50-Paper.pdf›, p. 2; Flournoy MA, Haines A and Chefitz G, 'Building Trust through Testing' (2020) ‹https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf›, p. 9.

[140] See Franz N, 'Targeted Killing and Pattern-of-Life Analysis: Weaponised Media' (2017) 39 Media, Culture & Society 111, 114

[141] See Corrin A, 'Sensory Overload: Military Is Dealing with

Looking at this from a legal angle, as soon as such algorithmic decision-making systems are deployed during situations of armed conflict in order to support or take targeting decisions, applicable international humanitarian law might indeed even prescribe such all-encompassing and highly intrusive data collection measures. Article 57(2)(a)(i) Additional Protocol I provides that "those who plan or decide upon an attack shall do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives (...) and that it is not prohibited by the provisions of this Protocol to attack them". Noting that this obligation comprises measures by intelligence agencies to properly analyse and verify targets prior to engagement,[142] Asaf Lubin has argued that the principle of precautions in attack as stipulated by Article 57(2) AP I dictates the establishment of a "reasonable intelligence agency" that is able to reliably verify the identity of targets prior to a strike.[143] If reliability in a machine-learning system can only – if at all – be achieved with unfettered collection of data relevant for the (geographic) area of deployment, then this would imply that IHL prescribes such practices.

As indicated above, these data are not necessarily exclusively personal. It will be as useful for an AI-supported targeting system or an UAV tasked with an ISR mission to be able to "recognise" a tank and to be able to distinguish it from a school bus. However, while personal data are perhaps less relevant in regard to near-peer conflicts that play out on the "digital battlefield", they are very much a defining feature of the "personalised warfare" of post-9/11 counterterrorism operations, in the context of which individuals instead of states have become "imminent threats". It is in this respect that the "military surveillance paradigm" has really manifested itself, enabled and reinforced by the development of novel digital technologies.[144] In regions where this type of conduct is mainly being carried out, operating militaries may claim that their strikes have become more precise, with fewer civilians ending up as "collateral damage".[145] However, it is easy to see how the paradigm can turn into a sophisticated yet sinister form of population control in affected areas, with constant multi-source surveillance creating a situation of "perpetual policing"[146] in which the resident civilian population is aware

a Data Deluge' (Defense Systems, 4 February 2010) ‹https://defensesystems.com/articles/2010/02/08/home-page-defense-military-sensors.aspx›.

[142] Lubin A, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law' in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives (2021) ‹https://papers.ssrn.com/sol3/papers.cfm?abstract*id=3622061›, p. 25, referring to Sandoz Y, Swinarski C and Zimmermann B, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (1987), p. 681.*

[143] See Lubin A, 'The Reasonable Intelligence Agency' (2021) 47 The Yale Journal of International Law ‹https://papers.ssrn.com/sol3/papers.cfm?abstract*id=3805700›.*

[144] See Bhuta N and Mignot-Mahdavi R, 'Dangerous Proportions: Means and Ends in Non-Finite War' (2021) Asser Research Paper 2021-01, p. 20-22.

[145] According to Israeli media outlets, this is precisely what happened during the latest IDF campaign in Gaza, thanks to the widespread use of machine-learning systems, see Gross JA, 'IDF Intelligence Hails Tactical Win in Gaza, Can't Say How Long Calm Will Last' The Times of Israel (27 May 2021) ‹https://www.timesofisrael.com/idf-intel-hails-tactical-win-over-hamas-but-cant-say-how-long-calm-will-last/›: "These advanced capabilities were used to sift through the unimaginably massive amounts of data that Military Intelligence intercepts and collects from Gaza — telephone calls, text messages, surveillance camera footage, satellite images and a huge array of various sensors — in order to turn them into usable intelligence information: where will a specific Hamas commander be located at a specific time, for instance. To give a sense of scale of the amount of data being collected, the IDF said it estimates that any given point in the Gaza Strip was photographed at least 10 times each day during the conflict. (...) This allowed Military Intelligence to not only kill several dozen top operatives from Hamas and the Palestinian Islamic Jihad, the second-most significant terror group in the Strip, but also to do so with a smaller number of civilian casualties."

[146] Franz N, 'Targeted Killing and Pattern-of-Life Analysis: Weaponised Media' (2017) 39 Media, Culture & Society 111, 112-114.

that any deviation from vaguely understood "normal behaviour" might result in a lethal drone strike, because some employed algorithm in an ISR or targeting system flagged said behaviour as likely terrorist activity.[147]

What emerges, then, is a genuine conflict of interests that appears to be largely unresolved: The rules of IHL seem to require, at least to some extent, the collection of large quantities of personal data in situations in which a machine-learning system is used to support a decision-making process that leads up to the employment of lethal force. This must encourage the sweeping up of data from all available sources to improve target identification. At the same time, for affected populations this implies that the right to privacy is effectively suspended. The ensuing question then becomes whether and how this fundamental human right can be meaningfully realised at all. For one, it is highly doubtful whether IHL provides for any type of data protection to protect an individual's privacy, at least as far as the conduct of hostilities is concerned.[148] As indicated in the previous section, this is perhaps of lesser relevance as most data collection will be conducted during peacetime anyway. However, the application of international human rights law, which in principle would be able to introduce certain procedural safeguards against limitless collecting and processing of sensitive personal data, faces numerous legal obstacles even if the issue of extraterritorial jurisdiction can be overcome, as recently suggested by the German Federal Constitutional Court.[149] Most importantly, most data protection regimes are subject to so-called national security exclusions that, as noted by Lubin, "would seem to block the relevance of much of the data protection legal framework to AI applications developed for and utilized in armed conflict, as well as any processing conducted by security and intelligence agencies".[150] Aside from that, it has been observed that current data protection regimes, most importantly the European General Data Protection Regulation, struggle to adequately account for the real challenges posed by algorithmic decision-making systems.[151] For the time being, then, the proliferation of AI systems in ISR and targeting as part of the "digital battlefield" seems not to face many legal hurdles, which means that the "military surveillance paradigm" will continue to prevail.

---

[147] How sloppy pattern recognition can end up killing civilians has been demonstrated many times over the course of the "war on terror", whether machine-learning systems had supported the decision to use force or not; see as a particularly striking example the botched drone strike against a putative ISIS-K member in Kabul on 29 August 2021, Aikins M, 'Times Investigation: In U.S. Drone Strike, Evidence Suggests No ISIS Bomb' The New York Times (10 September 2021) ‹https://www.nytimes.com/2021/09/10/world/asia/us-air-strike-drone-kabul-afghanistan-isis.html›.

[148] The situation differs in relation to, for example, the treatment of prisoners of war, which is not the subject of this paper.

[149] See 1 BvR 2835/17 (Federal Constitutional Court); to be sure, the case concerned the application of German Basic Law and not IHRL.

[150] Lubin A, 'Big Data and the Future of Belligerency: Applying the Rights to Privacy and Data Protection to Wartime Artificial Intelligence' in Robin Geiß and Henning Lahmann (eds), Research Handbook on Warfare and Artificial Intelligence (2022) ‹https://papers.ssrn.com/sol3/papers.cfm?abstract_*id_=3919195*›, *p. 9; the author points out that the EU draft proposal for AI regulation explicitly excludes systems developed for military purposes, see Proposal for the Regulation of the European Parliament and the Council Laying Down Harmonised Rules on*

Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Legislative Acts, COM/2021/206 final (Apr. 21, 2021).

[151] Dreyer S and Schulz W, 'The GDPR and Algorithmic Decision-Making' (Völkerrechtsblog, 3 June 2019) ‹https://voelkerrechtsblog.org/de/the-gdpr-and-algorithmic-decision-making/›; Dreyer S and Schulz W, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?' (Bertelsmann Stiftung 2019) ‹https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GDPR.pdf›.

3.3 THE SPATIAL AND TEMPORAL DISSOLUTION OF THE CONFLICT ZONE

Closely related to the previous two sections, a further consequence of the digital transformation of warfare is a creeping dissolution of the spatial and temporal boundaries of (armed) conflict. For one, this development can partly be interpreted as a conceptual extension of the global "war on terror", which – as mentioned above – led to an individualisation of warfare: digital technologies make permanent and globally unconstrained surveillance of persons possible, and the use of force against targets is largely decided on the basis of certain characteristics that designate individuals as imminent threats to the security of the acting power. This results in a constant anticipation of violence, which in turn prompts the state to act preemptively against the targeted individual.[152] In this sense, the global surveillance practices, and the increasing fusion of intelligence from various different sources, creates its own sense of infinite and ultimately unsolvable insecurity. As the past two decades have shown, this constant state of quasi-conflict leads to an increase in civilian casualties, mostly due to "over the horizon"[153] drone strikes and other types of remote warfare. But perhaps even more significantly, this strategy directly affects the well-being of the civilian populations in countries and areas where these missions are mainly carried out. With the increasing proliferation of AI-supported ISR and targeting technologies, there is no reason to believe that this type of low-key, deterritorialised and perpetual conflict will abate in the coming decades, as its execution will only become easier and thus further entrenched.

The negative effects stemming from constant surveillance might be less severe or even non-existent outside the context of the "war on terror" or other conflicts between states and transnational armed groups, i.e. as far as state-on-state conflict is concerned. But even here, the spatial and temporal dissolution of the conflict zone has increasingly begun to manifest as a consequence of novel digital means of military conduct, mainly due to a spread of offensive cyber activities that enable a persistent presence in adversarial networks, either for the purpose of intelligence gathering – which might involve the copying of sensitive and personal data of other states' civilian populations – or in order to "prepare the battlefield" as described above. These activities, too, are occurring during what is, from a legal perspective, appropriately conceived as "peacetime", yet it leads to a further blurring of the boundaries, leading in a constant state of quasi- or almost-conflict between states. Although mostly directed against governmental or official assets, it is important to note that this type of ongoing activity has potential repercussions for the civilian populations as well, for instance as a result of spying activities that affect personal data or even of network intrusions that accidentally damage critical civilian infrastructures, especially if the adversarial state employs indiscriminate offensive cyber tools such as self-propagating malware.[154] Moreover, the awareness that other states might constantly be present in one's own networks easily creates the impression of imminent danger and heightened vulnerability – not least given the fact that many new digital weapons technologies enable states to launch attacks faster – which gives states further incentive to respond in kind and collect more intelligence through offensive cyber conduct. This, in turn, might give rise to a feedback loop of ever-greater perception that the adversary presents a constant threat, a situation that bears

[152] Bhuta N and Mignot-Mahdavi R, 'Dangerous Proportions: Means and Ends in Non-Finite War' (2021) Asser Research Paper 2021-01, 20-22.

[153] Szymanski S and Marchman M, '"Over-the-Horizon Operations" in Afghanistan' (Articles of War, 8 September 2021) ‹https://lieber.westpoint.edu/over-the-horizon-operations-afghanistan/›.

[154] See e.g. the NotPetya malware, a cyber operation that caused immense damage in a number of countries without reaching the "armed conflict" threshold, Greenberg A, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' [2018] Wired ‹https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/›.

considerable risks of unintended escalation.

As explained in section 3.1, and as evidenced by the ongoing war on terror, the current international legal order has not demonstrated to be appropriately responsive to this type of perpetual, low-intensity warfare. Absent the applicability of international humanitarian law, some experts have argued for a more robust interpretation of peacetime rules that might be able to capture some of the novel kinds of military activities especially in cyberspace. But as mentioned, to date it remains highly contested whether notions such as "the rule of sovereignty",[155] the principle of non-intervention, or indeed international human rights law are capable of stepping in to provide adequate legal protection against some of the more reckless of such offensive cyber operations.

3.4 STATES' POSITIVE OBLIGATIONS CONCERNING VULNERABILITIES OF DIGITAL WARFARE TECHNOLOGIES

Observers have repeatedly pointed out that one of the most critical issues in the context of the digitalisation of the armed forces, especially with regard to AI-supported equipment, is the virtually inevitable introduction of considerable cyber vulnerabilities, with potentially far-reaching consequences.[156] It is beyond question that no code is ever written without flaws, and the more complex the software, the more likely it becomes that adversaries will be able to hack into and potentially sabotage these digital systems. When it comes to machine-learning algorithms, the malicious exploitation of such vulnerabilities can lead to unforeseeable and ultimately devastating consequences.[157] The ensuing risks are a function of the degree of complexity of the system.

For example, if soldiers in the field rely on a "battle management network" that employs fusion technologies to gather and streamline critical information about the current mission and an adversary gains access to the data streams through an offensive cyber operation, the latter might be in a position to alter the data in a way that results in a misleading picture of the tactical situation,[158] potentially putting civilians present in the theatre of conflict in harm's way. A "spoofing" attack that replaces a machine-learning system's incoming data feed with a fake one might lead an autonomous vehicle astray and act erroneously,[159] which can likewise result in harm to civilians or civilian objects. Such manipulation might even already happen during the algorithm's training stage by way of "data poisoning", that is the injection of directed, corrupted disinformation into datasets used for the training of the machine-learning system.[160] Attacking AI-supported ISR capabilities in this way might lead to a flood of false and untrustworthy intelligence reports that might inhibit a military commander's ability to make informed decisions during combat.[161] These risks

[155] See Schmitt MN (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017), rule 4.

[156] See Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021), p. 32.

[157] See Herpig S, 'Securing Artificial Intelligence. Part 1: The Attack Surface of Machine Learning and Its Implications' (Stiftung Neue Verantwortung 2019) ‹https://www.stiftung-nv.de/sites/default/files/securing*artificial*intelligence.pdf›.

[158] Zheng DE and Carter WA, 'Leveraging the Internet of Things for a More Efficient and Effective Military' (Center for Strategic & International Studies 2015) ‹https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy*files/files/publication/150915*Zheng*Leveragingthe*WEB.pdf›, p. 20.

[159] Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021), p. 7.

[160] Herpig S, 'Securing Artificial Intelligence. Part 1: The Attack Surface of Machine Learning and Its Implications' (Stiftung Neue Verantwortung 2019) ‹https://www.stiftung-nv.de/sites/default/files/securing*artificial*intelligence.pdf›, p. 16.

[161] Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

from vulnerabilities further increase when immensely complex AI infrastructures like autonomous swarms are involved, which depend on highly sophisticated and stable communication networks that are inherently vulnerable to "jamming, spoofing, hacking, hijacking, manipulation or other electronic warfare attacks".[162] As reported by Gady, military decision-makers seem well aware of these potentially extremely consequential vulnerabilities and do not expect the situation to change fundamentally any time soon.[163]

These example demonstrate that the increasing dependency on AI and other digital systems creates real risks not simply for the functioning of these battlefield infrastructures by way of adversarial cyber conduct aiming at disabling or neutralising them, which in itself would not raise any specific legal issues. Much more important for the context at hand is the very real possibility that machine-learning systems might be manipulated so that their behaviour is altered in unpredictable ways, in worst-case scenarios resulting in the erroneous targeting of civilians or other protected persons or objects. In light of the rapidly increasing digitalisation of military assets and more and more reliance on AI-supported systems, this poses a lasting and serious problem for the future of humanitarian protection.

States that employ these digital technologies in military systems have positive legal obligations to prevent the causation of harm to civilians and other protected persons and objects due to malfunction or erroneous behaviour as a result of an adversarial cyber operation against them. Different rules in international law exist as a basis for this type of obligation. For one, both the duty to test new weapons pursuant to Article 36 AP I and the principle of precautions in attack pursuant to Article 57 AP I contain provisions that address the risk of harm to civilians emanating from employed military systems. According to Article 36 AP I, a state is under an obligation to determine whether the employment of a new weapon, means or method of warfare would, in some or all circumstances, be prohibited by the Additional Protocol I or any other applicable rule of international law. Experts have repeatedly been advocating for the thorough application of this rule as a way to deal with the uncertainties of AI technologies in military assets.[164] However, the utility of such review mechanisms is arguably limited. When it comes to AI, it is already questionable whether it is ever possible to test a machine-learning system "in all possible scenarios and with all ranges of inputs".[165] It seems even more far-fetched to ever expect a review process to reveal all possible vulnerabilities in the system's source code that at some point in the future might be discovered and subsequently exploited by an adversary. The same holds true for the obligation stemming from Article 57(1) AP I to take constant care in the conduct of military operations to spare the civilian population, civilians and civilian objects. Even though the use of the notion "military operations" is broad enough to encompass all kinds of uses of AI in military applications – beyond the employment for the purpose of engaging targets, which as an "attack" is more specifically regulated in Article 57(2) AP I – it again cannot reasonably expected of a state to accurately predict all ways a machine-learning system might malfunction and harm civilians as the result of an adversarial cyber operation against the system.

Positive obligations can furthermore be found

[162] Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020), p. 54.

[163] See Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (IISS, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›.

[164] See Boulanin V and Verbruggen M, 'Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies' (Stockholm International Peace Research Institute 2017) ‹https://www.sipri.org/sites/default/files/2017-12/article*36*report*1712.pdf*›.

[165] Flournoy MA, Haines A and Chefitz G, 'Building Trust through Testing' (2020) ‹https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf›, p. 8.

in peacetime international law, most pertinently in international human rights law under the right to life, provided the issue of extraterritorial application can be overcome.[166] This, too, could potentially be interpreted as amounting to a duty to ensure that employed machine-learning systems cannot be manipulated in such a way as to render their behaviour uncontrollable and unpredictable, endangering the life of affected individuals. But whether or not such an obligation based on IHRL is accepted in principle, the applicable standard cannot be assumed to go beyond an obligation of observing due diligence, which would arguably not capture all hardly detectable, possible vulnerabilities in the system's software. The risk that an adversarial cyber attack leads to unpredictable malfunctioning of an AI system is, for the time being at least, virtually ineradicable.

3.5 HUMAN CONTROL: QUESTIONS PERTAINING TO ACCOUNTABILITY AND RESPONSIBILITY

Finally, urgent questions pertaining to the issue of (meaningful) human control over AI-supported military applications and a possible "accountability gap" resulting from certain features of these technologies, most significantly due to an inherent lack of predictability regarding the outcomes of dynamic processes by machine-learning algorithms,[167] have so far mostly been discussed more narrowly in the context of lethal autonomous weapons systems.[168] However, there is no reason not to expect these issues to resurface more broadly, for example when machine-learning systems support ISR or similar types of applications, in light of the fact that the amount of analysed data and the inherent opaqueness of the algorithmic processes will render effective human oversight and control oftentimes very difficult. The fundamental consideration how to achieve and guarantee meaningful human control is therefore no less important in contexts beyond LAWS – as explicitly acknowledged for example by the ICRC.[169]

The (otherwise persuasive) assertion that because any decision to employ an AI-supported system must ultimately have been made by an individual, human accountability always remains intact,[170] can perhaps solve the majority, but likely not all cases concerning unintended harm caused by an algorithm. Especially when it comes to the support of a human decision through the automatic processing and analysis of vast datasets, the ways in which actual human control takes a back seat may be subtle and perhaps even barely detectable. While in such scenarios, it might seem pretty straightforward to assign accountability to the human operator who had relied on the (faulty) automated analysis to take a critical decision, the uncomfortable truth may be that at some point, with ever-increasing amounts of data, humans simply do not retain the cognitive capabilities necessary to assess and evaluate the outcomes of an algorithmic process and can only put their trust in the reliability of the machine or abstain

[166] See only Milanovic M and Schmitt MN, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 Journal of National Security Law & Policy 247, 281-282.

[167] See Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021), p. 17-18.

[168] See only Verdriesen I, Santoni de Sio F and Dignum V, 'Accountability and Control Over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight' (2021) 31 Mind and Machines 137; Chengeta T, 'Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law' (2016) 45 Denver Journal of International Law & Policy 1.

[169] International Committee of the Red Cross, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach' (2019) ‹https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach›.

[170] See Bayley J, 'Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist, NATO' (Defence IQ, 30 July 2018) ‹https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data›.

from using it at all.[171] Here, the fundamental question remains how to re-establish the possibility of human control in the first place, a question that perhaps cannot be answered by taking a shortcut to default operator accountability. Therefore, much is left to discuss concerning this most critical aspect of the use of AI in the military.

4. CONCLUDING REMARKS

As this framing paper has demonstrated, while the development of the "future digital battlefield" might provide states with hitherto inconceivable opportunities to carry out highly sophisticated, effective, and potentially less lethal and destructive military operations, this does in no way mean that these come without serious risks for civilian populations. The third section has highlighted a few of the intricate legal questions in regard to future humanitarian protection that must urgently be asked as the digitalisation of warfare proceeds at a rapid pace. So far, few issues can be said to have been resolved and sincere debates must continue, not least among states, how to ensure that the future of military operations does not turn into complete dystopia. To that end, the paper may serve as a guideline for future legal, ethical, and political-science research that focuses on the convergent effects of the digital transformation rather than disparate subject matters such as disinformation campaigns or lethal autonomous weapons systems. Above all else, sections 3.1 to 3.3 have exposed the pressing need to tackle the primary issue of what legal regime is supposed to govern a wide variety of prospective military activities that involve potentially profound ramifications for affected civilian populations. With the emergence of the digital battlefield, the clear-cut distinction between war and peace that is at the root of international humanitarian law is fast becoming obsolete once again, and the broader system of international law must prove responsive to this development so as to remain relevant for the regulation of states' conduct of warfare.

[171] See Herpig S, 'Securing Artificial Intelligence. Part 1: The Attack Surface of Machine Learning and Its Implications' (Stiftung Neue Verantwortung 2019) ‹https://www.stiftung-nv.de/sites/default/files/securing*artificial*intelligence.pdf›, p. 35: "If a human follows through with a decision based on an analysis provided by machine learning, how much transparency about this analysis is needed and where will this require unconditional trust that the analysis is correct and was not interfered with?"

BIBLIOGRAPHY

- Afina Y, 'Rage Against the Algorithm: The Risks of Overestimating Military Artificial Intelligence' (*Chatham House*, 27 August 2020) ‹https://www.chathamhouse.org/2020/08/rage-against-algorithm-risks-overestimating-military-artificial-intelligence›
- Ahronheim A, 'Israel's Operation against Hamas Was the World's First AI War' *The Jerusalem Post* (27 May 2021) ‹https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371›
- Aikins M, 'Times Investigation: In U.S. Drone Strike, Evidence Suggests No ISIS Bomb' *The New York Times* (10 September 2021) ‹https://www.nytimes.com/2021/09/10/world/asia/us-air-strike-drone-kabul-afghanistan-isis.html›
- Barnett J, 'Air Force Moving Project Maven into Advanced Battle Management System Portfolio' (*FedScoop*, 10 August 2020) ‹https://www.fedscoop.com/project-maven-air-forces-advanced-battle-management-system/›
- ——, 'Latest ABMS Tests Break New Barriers on AI and Edge Cloud Capabilities' (*FedScoop*, 18 March 2021) ‹https://www.fedscoop.com/latest-abms-tests-ai-cloud-cybersecurity/›
- Barrie D and Childs N, 'Air Power's Future: Combat Aircrew Not yet Surplus to Requirements' (*IISS Military Balance Blog*, 24 July 2020) ‹https://www.iiss.org/blogs/military-balance/2020/07/air-power-future-autonomous-platforms›
- Bayley J, 'Transforming ISR Capabilities through AI, Machine Learning and Big Data: Insights from Dr. Thomas Killion, Chief Scientist, NATO' (*Defence IQ*, 30 July 2018) ‹https://www.defenceiq.com/defence-technology/news/transforming-isr-capabilities-through-ai-machine-learning-and-big-data›
- Ben-Yishai R, 'How Data and AI Drove the IDF Operation in Gaza' *YNet News* (29 May 2021) ‹https://www.ynetnews.com/magazine/article/SJ2rHS6Y00›
- Bergman R and Fassihi F, 'The Scientist and the A.I.-Assisted, Remote-Control Killing Machine' *The New York Times* (18 September 2021) ‹https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html?referringSource=articleShare›
- Bhuta N and Mignot-Mahdavi R, 'Dangerous Proportions: Means and Ends in Non-Finite War' (2021) Asser Research Paper 2021-01
- Boulanin V and Verbruggen M, 'Article 36 Reviews: Dealing with the Challenges Posed by Emerging Technologies' (Stockholm International Peace Research Institute 2017) ‹https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf›
- Bronk C and Anderson GS, 'Encounter Battle: Engaging ISIL in Cyberspace' (2017) 2 The Cyber Defense Review 93
- Bronk J, 'Technological Trends' in Peter Roberts (ed), *The Future Conflict Operating Environment Out to 2030* (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906_op_future_operating_enviroment_web.pdf›

- Buchanan B and Cunningham FS, 'Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis' (2020) 3 Texas National Security Review 54
- Çalı B, 'Has "Control over Rights Doctrine" for Extra-Territorial Jurisdiction Come of Age? Karlsruhe, Too, Has Spoken, Now It's Strasbourg's Turn' (*EJIL: Talk!*, 21 July 2020) ‹https://www.ejiltalk.org/has-control-over-rights-doctrine-for-extra-territorial-jurisdiction-come-of-age-karlsruhe-too-has-spoken-now-its-strasbourgs-turn/›
- Cavoukian A, 'Global Privacy and Security, by Design: Turning the "Privacy vs. Security" Paradigm on Its Head' (2017) 7 Health Technologies 329
- CBS News, 'Israel Claims 200 Attacks Predicted, Prevented with Data Tech' *CBS News* (12 June 2018) ‹https://www.cbsnews.com/news/israel-data-algorithms-predict-terrorism-palestinians-privacy-civil-liberties/›
- Chahal H, Fedasiuk R and Flynn C, 'Messier than Oil: Assessing Data Advantage in Military AI' (Center for Security and Emerging Technology 2020)
- Chengeta T, 'Accountability Gap: Autonomous Weapon Systems and Modes of Responsibility in International Law' (2016) 45 Denver Journal of International Law & Policy 1
- Corrin A, 'Sensory Overload: Military Is Dealing with a Data Deluge' (*Defense Systems*, 4 February 2010) ‹https://defensesystems.com/articles/2010/02/08/home-page-defense-military-sensors.aspx›
- Crabtree J, 'Gaza and Nagorno-Karabakh Were Glimpses of the Future of Conflict' [2021] *Foreign Policy* ‹https://foreignpolicy.com/2021/06/21/gaza-nagorno-karabakh-future-conflict-drones/›
- Cramer M, 'A.I. Drone May Have Acted on Its Own in Attacking Fighters, U.N. Says' *The New York Times* (3 June 2021) ‹https://www.nytimes.com/2021/06/03/world/africa/libya-drone.html›
- Dar Y, 'Israel Says It Fought World's First "Artificial Intelligence War" Against Hamas' *The Eurasian Times* (29 May 2021) ‹https://eurasiantimes.com/israel-sys-it-fought-worlds-first-artificial-intelligence-war-against-hamas/›
- Defense Intelligence Agency, 'Challenges to Security in Space' (2019) ‹https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf›
- Delerue F, *Cyber Operations and International Law* (2020)
- Dorsey J and Amaral N, 'Military Drones in Europe: Ensuring Transparency and Accountability' (Chatham House 2021) ‹https://www.chathamhouse.org/sites/default/files/2021-04/2021-04-30-military-drones-europe-dorsey-amaral.pdf›
- ——, 'Transparency, Accountability and Legitimacy—Chatham House Report on Military Drones in Europe, Part I' (*Opinio Juris*, 21 May 2021) ‹http://opiniojuris.org/2021/05/21/transparency-accountability-and-legitimacy-chatham-house-report-on-military-drones-in-europe-part-i/›
- Dreyer S and Schulz W, 'The General Data Protection Regulation and Automated Decision-Making: Will It Deliver?' (Bertelsmann Stiftung 2019) ‹https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/GDPR.pdf›
- ——, 'The GDPR and Algorithmic Decision-Making' (*Völkerrechtsblog*, 3 June 2019) ‹https://voelkerrechtsblog.org/de/the-gdpr-and-algorithmic-decision-making/›

- Dunhill J, 'First "AI War": Israel Used World's First AI-Guided Swarm Of Combat Drones In Gaza Attacks' *IFL Science* (2 July 2021) ‹https://www.iflscience.com/technology/first-ai-war-israel-used-worlds-first-aiguided-swarm-of-combat-drones-in-gaza-attacks/›
- Ekelhof M and Persi Paoli G, 'Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems' (United Nations Institute for Disarmament Research 2020)
- Emanuel P and others, 'Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD'
- Evans JC, 'Hijacking Civil Liberties: The USA PATRIOT Act of 2001' (2002) 33 Loyola University Chicago Law Journal 933
- Fischerkeller MP and Harknett RJ, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation' [2019] The Cyber Defense Review 267
- Flournoy MA, Haines A and Chefitz G, 'Building Trust through Testing' (2020) ‹https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf›
- Franz N, 'Targeted Killing and Pattern-of-Life Analysis: Weaponised Media' (2017) 39 Media, Culture & Society 111
- Frisk A, 'What Is Project Maven? The Pentagon AI Project Google Employees Want out Of' (*Global News*, 5 April 2018) ‹https://globalnews.ca/news/4125382/google-pentagon-ai-project-maven/›
- Gady F-S, 'What Does AI Mean for the Future of Manoeuvre Warfare?' (*IISS*, 5 May 2020) ‹https://www.iiss.org/blogs/analysis/2020/05/csfc-ai-manoeuvre-warfare›
- Gady F-S and Stronell A, 'What the Nagorno-Karabakh Conflict Revealed About Future Warfighting' (*World Politics Review*, 19 November 2020) ‹https://www.worldpoliticsreview.com/articles/29229/what-the-nagorno-karabakh-conflict-revealed-about-future-warfighting›
- Geiß R and Lahmann H, 'Protection of Data in Armed Conflict' (2021) 97 International Law Studies 556
- ——, 'Protecting Societies - Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchori.pdf›
- ——, 'Protecting the Global Information Space in Times of Armed Conflict' (Geneva Academy of International Humanitarian Law and Human Rights 2021) ‹https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf›
- Greenberg A, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' [2018] *Wired* ‹https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/›
- Greenwald G, 'Inside the Mind of NSA Chief Gen Keith Alexander' *The Guardian* (15 September 2013) ‹https://www.theguardian.com/commentisfree/2013/sep/15/nsa-mind-keith-alexander-star-trek›
- Gross JA, 'IDF Intelligence Hails Tactical Win in Gaza, Can't Say How Long Calm Will Last' *The*

Times of Israel (27 May 2021) ‹https://www.timesofisrael.com/idf-intel-hails-tactical-win-over-hamas-but-cant-say-how-long-calm-will-last/›

- ——, 'In Apparent World First, IDF Deployed Drone Swarms in Gaza Fighting' *The Times of Israel* (10 July 2021) ‹https://www.timesofisrael.com/in-apparent-world-first-idf-deployed-drone-swarms-in-gaza-fighting/›
- Hammes TX, 'The Future of Warfare: Small, Many, Smart vs. Few & Exquisite?' (*War on the Rocks*, 16 July 2014) ‹https://warontherocks.com/2014/07/the-future-of-warfare-small-many-smart-vs-few-exquisite/›
- Harris M, 'Phantom Warships Are Courting Chaos in Conflict Zones' [2021] *Wired* ‹https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/?utm_source=pocket_mylist›
- Herpig S, 'Securing Artificial Intelligence. Part 1: The Attack Surface of Machine Learning and Its Implications' (Stiftung Neue Verantwortung 2019) ‹https://www.stiftung-nv.de/sites/default/files/securing_artificial_intelligence.pdf›
- Hickman PL, 'The Future of Warfare Will Continue to Be Human' (*War on the Rocks*, 12 May 2020) ‹https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/›
- Hoffman S, 'The U.S.-China Data Fight Is Only Getting Started' [2021] *Foreign Policy* ‹https://foreignpolicy.com/2021/07/22/data-tiktok-china-us-privacy-policies/?utm_source=pocket_mylist›
- Hoffman S and Attrill N, 'Supply Chains and the Global Data Collection Ecosystem' (Australian Strategic Policy Institute 2021) Policy Brief 45/2021 ‹https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-06/Supply%20chains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92ADaZH›
- Holland Michel A, 'Known Unknowns: Data Issues and Military Autonomous Systems' (United Nations Institute for Disarmament Research 2021)
- ——, 'There Are Spying Eyes Everywhere – And Now They Share a Brain' [2021] *Wired* ‹https://www.wired.com/story/there-are-spying-eyes-everywhere-and-now-they-share-a-brain/›
- Horowitz MC and others, 'Artificial Intelligence and International Security' (Center for a New American Security 2018) ‹https://s3.amazonaws.com/files.cnas.org/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf›
- International Committee of the Red Cross, 'Autonomous Weapon Systems: Is It Morally Acceptable for a Machine to Make Life and Death Decisions?' (*ICRC*, 13 April 2015) ‹https://www.icrc.org/en/document/lethal-autonomous-weapons-systems-LAWS›
- ——, 'Autonomy, Artificial Intelligence and Robotics: Technical Aspects of Human Control' (2019)
- ——, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2019)
- ——, 'The Potential Human Cost of Cyber Operations' (2019) ‹https://www.icrc.org/en/document/potential-human-cost-cyber-operations›
- ——, 'Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach' (2019) ‹https://www.icrc.org/en/document/artificial-intelligence-and-machine-

learning-armed-conflict-human-centred-approach›

- ——, 'The Potential Human Cost of the Use of Weapons in Outer Space and the Protection Afforded by International Humanitarian Law. Position Paper Submitted by the International Committee of the Red Cross to the Secretary-General of the United Nations on the Issues Outlined in General Assembly Resolution 75/36' (2021)
- Jensen BM, Whyte C and Cuomo S, 'Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence' (2020) 22 International Studies Review 526
- Kaltheuner F and Bietti E, 'Data Is Power: Towards Additional Guidance on Profiling and Automated Decision-Making in the GDPR' (2018) 2 Journal of Information Rights, Policy and Practice ‹http://doi.org/10.21039/irpandp.v2i2.45›
- Konaev M, 'With AI, We'll See Faster Fights, But Longer Wars' (*War on the Rocks*, 29 October 2019) ‹https://warontherocks.com/2019/10/with-ai-well-see-faster-fights-but-longer-wars/›
- Kumon T, 'The First AI Conflict? Israel's Gaza Operation Gives Glimpse of Future' *Nikkei Asia* (28 June 2021) ‹https://asia.nikkei.com/Politics/International-relations/The-first-AI-conflict-Israel-s-Gaza-operation-gives-glimpse-of-future›
- Lahmann H, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' [2021] Duke Journal of Comparative & International Law
- Lawson E, 'Into the Ether: Considering the Impact of the Electromagnetic Environment and Cyberspace on the Operating Environment' in Peter Roberts (ed), *The Future Conflict Operating Environment Out to 2030* (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906_op_future_operating_enviroment_web.pdf›
- Lawson E and Mačák K, 'Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict' (International Committee of the Red Cross 2021)
- Lewis DA, 'Legal Reviews of Weapons, Means and Methods of Warfare Involving Artificial Intelligence: 16 Elements to Consider' (*ICRC Humanitarian Law & Policy*, 21 March 2019) ‹https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/›
- Lubin A, 'The Reasonable Intelligence Agency' (2021) 47 The Yale Journal of International Law ‹https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3805700›
- ——, 'The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law' in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives* (2021) ‹https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3622061›
- ——, 'Big Data and the Future of Belligerency: Applying the Rights to Privacy and Data Protection to Wartime Artificial Intelligence' in Robin Geiß and Henning Lahmann (eds), *Research Handbook on Warfare and Artificial Intelligence* (2022) ‹https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3919195›
- Makewar A, 'Israel Used First-Ever AI-Guided Combat Drone Swarm in Gaza Attacks' (6 July 2021) ‹https://www.inceptivemind.com/israel-used-first-ever-ai-guided-combat-drone-swarm-gaza-attacks/19940/›
- Margulies J, '9/11 Forever' [2021] *The Boston Review* ‹https://bostonreview.net/war-

security/joseph-margulies-911-forever›

- Margulies J and Azmy B, 'The Humanity of Michael Ratner, The Fabrications of Samuel Moyn' (*Just Security*, 13 September 2021) ‹https://www.justsecurity.org/78204/the-humanity-of-michael-ratner-the-fabrications-of-samuel-moyn/?utm_source=pocket_mylist›
- Mégret F, 'Are There "Ineherently Sovereign Functions" in International Law?' (2021) 115 American Journal of International Law 452
- Milanovic M, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal 81
- Milanovic M and Schmitt MN, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 Journal of National Security Law & Policy 247
- Miller RA, 'The German Constitutional Court Nixes Foreign Surveillance' (*Lawfare*, 27 May 2020) ‹https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance›
- Moynihan H, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention' (2019) ‹https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf›
- National Reconnaissance Office, 'NRO Key Talking Points: Sentient' (September 2016) ‹https://www.nro.gov/Portals/65/documents/foia/declass/ForAll/051719/F-2018-00108_C05112983.pdf›
- Park D and Walstrom M, 'Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks' (*The Henry M. Jackson School of International Studies*, 11 October 2017) ‹https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/›
- Pethokoukis J, 'How AI Is like That Other General Purpose Technology, Electricity' (*AEIdeas*, 25 November 2019) ‹https://www.aei.org/economics/how-ai-is-like-that-other-general-purpose-technology-electricity/›
- Reed J, Routh A and Mariani J, 'Information at the Edge: A Space Architecture for a Future Battle Network' (*Deloitte Insights*, 16 November 2020) ‹https://www2.deloitte.com/us/en/insights/industry/public-sector/future-space-weapons-space-architecture.html›
- Reinke B, 'Rights Reaching beyond Borders' (*Verfassungsblog*, 30 May 2020) ‹https://verfassungsblog.de/rights-reaching-beyond-borders/›
- Royal Marines, 'Drone Swarms Support Commando Forces Trials in a First for the UK's Armed Forces' (*Royal Navy*, 17 July 2021) ‹https://www.royalnavy.mod.uk/news-and-latest-activity/news/2021/july/17/210715-autonomous-advance-force-4›
- Sandoz Y, Swinarski C and Zimmermann B, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (1987)
- Sauer F, 'Autonomy in Weapons Systems: Playing Catch up with Technology' (*ICRC Humanitarian Law & Policy*, 29 September 2021) ‹https://blogs.icrc.org/law-and-policy/2021/09/29/autonomous-weapons-systems-technology/›
- Scharre P, 'Between a Roomba and a Terminator: What Is Autonomy?' (*War on the Rocks*, 18

February 2015) ‹https://warontherocks.com/2015/02/between-a-roomba-and-a-terminator-what-is-autonomy/›

- ——, 'Robots at War and the Quality of Quantity' (*War on the Rocks*, 26 February 2015) ‹https://warontherocks.com/2015/02/robots-at-war-and-the-quality-of-quantity/›
- ——, 'Unleash the Swarm: The Future of Warfare' (*War on the Rocks*, 4 March 2015) ‹https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/›
- Schmitt MN (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017)
- Schultz RH and Clarke RD, 'Big Data at War: Special Operations Forces, Project Maven, and Twenty-First Century Warfare' (*Modern War Institute*, 25 August 2020) ‹https://mwi.usma.edu/big-data-at-war-special-operations-forces-project-maven-and-twenty-first-century-warfare/›
- Scoles S, 'It's Sentient: Meet the Classified Artificial Brain Being Developed by US Intelligence Programs' [2019] *The Verge* ‹https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai›
- Shereshevsky Y, 'Are All Soldiers Created Equal? – On the Equal Application of the Law to Enhanced Soldiers' (2021) 61 Virginia Journal of International Law 271
- Smagh NS, 'Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition' (Congressional Research Service 2020) R46389 ‹https://fas.org/sgp/crs/intel/R46389.pdf›
- Stacey E, 'The Future of Cyber Warfare – An Interview with Greg Austin' (*Strife*, 26 April 2020) ‹https://www.strifeblog.org/2020/04/26/the-future-of-cyber-warfare-an-interview-with-greg-austin/›
- ——, 'Future Warfighting in the 2030s: An Interview with Franz-Stefan Gady' (*Strife*, 9 September 2020) ‹https://www.strifeblog.org/2020/09/09/future-warfighting-in-the-2030s-an-interview-with-franz-stefan-gady/›
- Stickings A, 'Space, Strategic Advantage and Control of the Military High Ground' in Peter Roberts (ed), *The Future Conflict Operating Environment Out to 2030* (RUSI 2019) ‹https://rusieurope.eu/sites/default/files/201906_op_future_operating_enviroment_web.pdf›
- Stumborg M, 'See You in a Month: AI's Long Data Tail' (*War on the Rocks*, 17 October 2019) ‹https://warontherocks.com/2019/10/see-you-in-a-month-ais-long-data-tail/›
- Szymanski S and Marchman M, '"Over-the-Horizon Operations" in Afghanistan' (*Articles of War*, 8 September 2021) ‹https://lieber.westpoint.edu/over-the-horizon-operations-afghanistan/›
- Taori R and others, 'Measuring Robustness to Natural Distribution Shifts in Image Classification', *34th Conference on Neural Information Processing Systems* (2020) ‹https://proceedings.neurips.cc/paper/2020/file/d8330f857a17c53d217014ee776bfd50-Paper.pdf›
- Temple-Raston D, 'How the U.S. Hacked ISIS' (*NPR*, 26 September 2019) ‹https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis›
- The Economist, 'Open-Source Intelligence Challenges State Monopolies on Information' [2021] *The Economist* ‹https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information›
- Thornton R and Miron M, 'The Advent of the "Third Revolution in Military Affairs"; Is the UK

Now Facing the Threat of AI-Enabled Cyber Warfare(?)' (*Defence-In-Depth*, 21 July 2020) ‹https://defenceindepth.co/2020/07/21/the-advent-of-the-third-revolution-in-military-affairs-is-the-uk-now-facing-the-threat-of-ai-enabled-cyber-warfare/›

- Toomey P, 'Caught In the Internet: For the NSA, Phones Were Only the Beginning' [2015] *Foreign Affairs* ‹https://www.foreignaffairs.com/articles/2015-08-20/caught-internet›
- UN Human Rights Committee, 'General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life' (2018) CCPR/C/GC/36
- UN Security Council, 'Letter Dated 8 March 2021 from the Panel of Experts on Libya Established Pursuant to Resolution 1973 (2011) Addressed to the President of the Security Council' (UN Security Council 2021) S/2021/229 ‹https://undocs.org/S/2021/229›
- van der Waag-Cowling N, 'Stepping into the Breach: Military Responses to Global Cyber Insecurity' (*ICRC Humanitarian Law & Policy*, 17 June 2021) ‹https://blogs.icrc.org/law-and-policy/2021/06/17/military-cyber-insecurity/›
- Verdriesen I, Santoni de Sio F and Dignum V, 'Accountability and Control Over Autonomous Weapon Systems: A Framework for Comprehensive Human Oversight' (2021) 31 Mind and Machines 137
- Vergun D, 'Experts Predict Artificial Intelligence Will Transform Warfare' (*DoD News*, 5 June 2020) ‹https://www.defense.gov/Explore/News/Article/Article/2209480/experts-predict-artificial-intelligence-will-transform-warfare/›
- Villasenor J, 'How to Deal with AI-Enabled Disinformation' (*Brookings*, 23 November 2020) ‹https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/›
- Walch K, 'Is AI Overhyped?' [2020] *Forbes* ‹https://www.forbes.com/sites/cognitiveworld/2020/06/04/is-ai-overhyped/?sh=198613ee63ee›
- Wareham M, 'Stopping Killer Robots. Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control' (Human Rights Watch 2020) ‹https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and#›
- Warrell H, 'UK Targeted ISIS Drones and Online Servers in Cyber Attack' *Financial Times* (7 February 2021) ‹https://www.ft.com/content/360a8e1c-b241-40f7-b944-45a4f8854ac5›
- Winkler JD and others, 'Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense' (RAND Corporation 2019)
- Work J, 'The American Way of Cyber Warfare and the Case of ISIS' (*Atlantic Council*, 17 September 2019) ‹https://www.atlanticcouncil.org/blogs/new-atlanticist/the-american-way-of-cyber-warfare-and-the-case-of-isis/›
- Zetter K, 'NATO Researchers: Stuxnet Attack on Iran Was Illegal "Act of Force"' (*Wired*, 25 March 2013) ‹http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/›
- Zheng DE and Carter WA, 'Leveraging the Internet of Things for a More Efficient and Effective Military' (Center for Strategic & International Studies 2015) ‹https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf›
- Zimmermann A, 'Stop Building Bad AI' [2021] *Boston Review* ‹https://bostonreview.net/science-

nature/annette-zimmermann-stop-building-bad-ai?utm_source=Boston+Review+Email+Subscribers&utm_campaign=66efccfe63-MC_Newsletter_7_21_21&utm_medium=email&utm_term=0_2cb428c5ad-66efccfe63-41268478&mc_cid=66efccfe63&mc_eid=c319e80a73›

- Zuboff S, 'Be the Friction - Our Response to the New Lords of the Ring' *Frankfurter Allgemeine Zeitung* (25 June 2013) ‹https://www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html›
- ——, *The Age of Surveillance Capitalism* (2019)
- *Federal Trade Commission v Facebook, Inc* [2021] Federal District Court for the District of Columbia 1:20-cv-03590-JEB
- *1 BvR 2835/17* (Federal Constitutional Court)

The Geneva Academy of International Humanitarian Law and Human Rights

The Geneva Academy provides post-graduate education, conducts academic legal research and policy studies, and organizes training courses and expert meetings. We concentrate on branches of international law that relate to situations of armed conflict, protracted violence, and protection of human rights.

The Geneva Academy of International
Humanitarian Law and Human Rights

Villa Moynier
Rue de Lausanne 120B
CP 1063 - 1211 Geneva 1 - Switzerland
Phone: +41 (22) 908 44 83
Email: info@geneva-academy.ch
www.geneva-academy.ch