

Emerging Disruptive Technologies - Challenges for Arms Control

The military use of certain emerging technologies not only has the potential to revolutionise warfare, but also to cause disruption on the international stage. At the same time, traditional arms control measures have little or no effect. New approaches are needed but discussion on the issue has so far been limited.

- 2 Introduction to Emerging and Disruptive Technologies: Basic Concepts
- 3 Uncrewed military systems
- 8 Autonomy in weapons systems
- 13 Artificial intelligence and quantum computing
- 17 3D printing, Nanotechnology and Human Enhancement
- 21 Arms control and EDT – new concepts, new opportunities?
- 23 The EU and emerging technologies

Niklas Schoernig

Peace Research Institute Frankfurt (PRIF)

Frank Sauer

Bundeswehr University Munich

Cite as: Niklas Schoernig and Frank Sauer, "Emerging Disruptive Technologies - Challenges for Arms Control" in EUNPDC eLearning, ed. Niklas Schoernig, Peace Research Institute Frankfurt. Available at <https://eunpdc-elearning.netlify.app/lu-15/>, last modified 3 July 2025

The EU Non-Proliferation and Disarmament eLearning Course aims to cover all aspects of the EU non-proliferation and disarmament agenda. It's produced by PRIF with financial assistance of the European Union. The contents of individual learning units are the sole responsibility of the respective authors and don't necessarily reflect the position of the European Union.



Funded by
the European Union

1. Introduction to Emerging and Disruptive Technologies: Basic Concepts

A message from the author

The term 'emerging disruptive technologies' has gained some prominence in the military debate over the last couple of years. Generally speaking, emerging and disruptive technologies refer to new and innovative advancements with the potential to significantly impact their respective fields of application. Depending on who you ask, between six and fourteen technologies that are relevant from a military perspective are usually described as 'emerging'. These technologies include, amongst others, uncrewed remotely piloted systems, robotics, hypersonics, autonomy, artificial intelligence, quantum computing and sensing, additive manufacturing (also known as 3D printing), nanotechnology and materials, different forms of what has been termed 'human enhancement', biotechnology, and the latest developments in space. Obviously not all technologies mentioned are at the same stage in their development and while some have already been fielded (e.g. hypersonics), others are very early in the research and development cycle (e.g. quantum computing).

However, not all technologies seen as being of potential military relevance in the future are also 'disrupting'. The term 'disruptive innovation' was coined by the late economist Clayton Christensen in the 1990s to describe a new technology developed by a small actor, challenging the established big players by creating new markets and displacing old ones.^[1] One example is solid state drives with fast flash memory, which have almost completely displaced the market for classic magnetic hard drives. SSDs are not only much more robust against physical influences, but can now also be manufactured at low cost.



Solid State Drive
Jacek Halicki/Wikimedia Commons, CC BY-SA 4.0

Transferred to the international system, disruptive technologies do have the potential to completely overthrow the established power-based order, allowing smaller states to 'leapfrog' their stronger competitors.

Uncrewed remotely piloted systems, robotics and artificial intelligence (AI), which are enabling autonomy in weapons systems in more and more contexts, can be seen as disruptive developments in the military realm. Quantum computing is currently shaping up to be another example, with potentially wide-ranging implications for encryption methods and thus all kinds of secure and private digital communication.

What can be seen, however, is that while most emerging disruptive technologies do indeed have the potential to alter and reshape the battlefield of the future, it is very hard to apply traditional arms control concepts from the Cold War to these technologies. That said, so far no one has had the revolutionary idea of rethinking arms control for these technologies either.

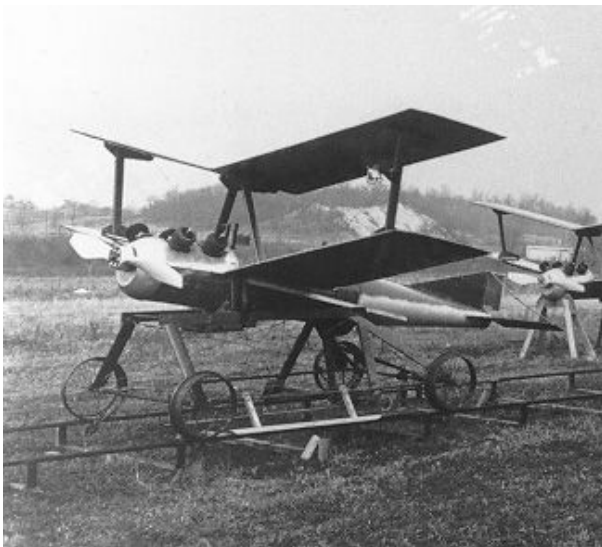
Before we debate a number of EDTs in more detail, one remark: In this learning unit, we will focus on a selection of emerging disruptive technologies only, as other learning units also offer relevant information on specific EDTs. For example, you will find information on hypersonic glide vehicles in the unit on missiles (LU07) [/1u-07/] or details on the latest developments in biotechnology in LU03 [/1u-03/].

1. Christensen, Clayton M. 2016: The Innovators Dilemma. Harvard Business Review Press

2. Uncrewed military systems

The long history of the uncrewed system

Technologies for remotely piloted military vehicles date back as far as World War I. A very early predecessor to today's remotely piloted aerial vehicles – commonly known as drones – was the British Kettering Bug shown here. It was initially launched without additional guidance, making it somewhat comparable to a cruise missile. Later on, attempts were made to fly the Kettering Bug by radio control, like a drone.



Kettering Bug (ca. 1918)
Wikimedia Commons/Public Domain

Back then, these systems were way too imprecise and unreliable to be of any use for defeating enemy targets. In fact, the early 20th century drones ended up as targets for shooting practice. It was not until the Vietnam era that drones eventually became valuable aerial reconnaissance and surveillance assets.



Vietnam-era drone (1969)
Wikimedia Commons/Public Domain

In recent decades, uncrewed systems have seen increasing military use. Examples include not only unmanned aerial vehicles (UAVs), but also unmanned

systems on and below the surface of the sea, as well as ground-based robots (UGVs).

The increased availability of uncrewed systems has brought significant changes to warfare, especially when it comes to dirty, dull or dangerous missions. These systems provide increased reconnaissance, surveillance and targeting capabilities, whilst allowing military personnel to stay out of harm's way. Moreover, unmanned systems can operate in hazardous environments, such as minefields, with the ability to operate around the clock, staying on mission for extended periods and providing real-time data and intelligence.



US Marines testing the 'Legged Squad Support System (LS3)'.
US DoD/Sgt. Sarah Dietz

Two technologies – GPS and satellite communication uplinks – significantly improved UAV capabilities towards the end of the 20th century, making it possible for them to be piloted with precision and from a great distance.



Grübelfabrik, CC BY-NC-SA

The well-known MQ-1 Predator, for instance, was already used for reconnaissance in the Balkan wars of the 1990s.



Armed MQ-1 Predator (2008)
US Air Force

Technological developments alone were not what gave rise to 'drone warfare', however. The political landscape was key. A major driver was 9/11 and the targeting of specific individuals during the so-called 'war on terror'. [1]

It is worth noting that commercial technology fueled this development – and so, today, we see not only military drones but countless civilian drones in all shapes and sizes, too. Russia's war against Ukraine is characterised by the use of an unprecedented number of remotely piloted vehicles, including both expensive weapons platforms and attritable one-way systems, many of the latter being repurposed commercial off-the-shelf quadcopters

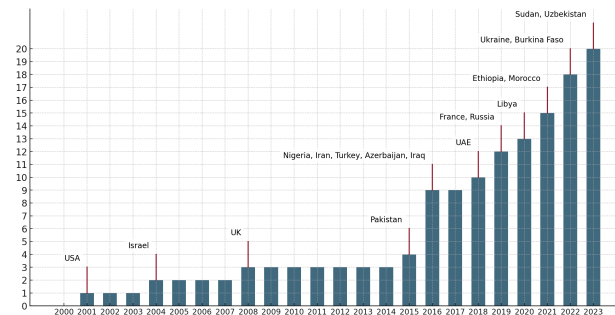


Weaponized commercial drone in Ukraine
www.mil.gov.ua, CC BY 4.0

The current state of drone proliferation and regulation

When it comes to proliferation, it has become almost impossible to keep track of which country has procured military drones, at least when working with unclassified sources. Many projects that at least tried to keep tabs on the situation, have stopped operating, including the renowned "World of Drones" project, run by the New America Foundation [2]. Who knows where the next container with Shaheds, Orlans or ZT-180s will end up? We do not know and we will not know, so we should not create the impression that we somehow

do. However, it is fair to assume that more than 100 countries have developed and/or procured military drones so far and that around 40 were in possession armed drones in the early 2020s. [3] Even tracking those countries which used armed drones in combat has become difficult, to say the least. As the following chart shows, up until the mid-2010s, only a handful of countries actively used combat drones, but since then, more and more states have been using these weapons. It is fair to say that drones have become a rather common sight on the battlefields worldwide and that classifying them as an 'emerging technology' is a bit of a stretch.



Countries having conducted drone strikes over time

Graphic created with the help of ChatGPT. Data: own collection, see below (Footnote #5)

[4]

The success of the military drone is partly due to the fact that in the 2000s, when not many countries were using this technology, which at the time was still new, it was not possible to introduce international restrictions let alone a ban on the use of military drones. Only a few arms control or export control regimes mention uncrewed vehicles explicitly. Another reason was the advent of new drone manufacturers such as China and Turkey. To understand the rise of these manufacturers, we have to look at what is (still) the most relevant regime covering military drones – the Missile Technology Control Regime (MTCR, also see LU12) [1/1u-12/]. [5] The MTCR is, according to its website, 'an informal political understanding' among 35, mostly Western states 'that seek to limit the proliferation of missiles and missile technology'. When the regime was formed in 1987, unmanned aerial vehicles were included as at that time people expected drones to serve as yet another delivery vehicle for weapons of mass destruction, rather than a cheap platform for conventional ammunition. For the USA in particular, however, the MTCR was, for a long time, one of the main hurdles to the export of military drones, which meant that only its closest allies, such as the UK, were allowed to import state-of-the-art drones such as the Predator or Reaper. But this opened opportunities for non-MTCR-member China to sell its drones worldwide while creating dependencies. Turkey, on the other hand, started developing its own drone industry after being unable to import US models, becoming one of the most in-demand drone producers in the world. In 2020, however, the US government decided to

reinterpret the MTCR guidelines to allow more US combat drones to fall into the less restrictive category III[6].

Other regimes worth mentioning in this context are the Arms Trade Treaty (ATT), the Wassenaar Arrangement, the Treaty on Conventional Armed Forces in Europe (CFE Treaty) and the Intermediate-Range Nuclear Forces (INF) Treaty see LU12 [1u-12/].

International treaties and regimes relevant for uncrewed systems

Missile Technology Control Regime (MTCR)

Missile Technology Control Regime

[<https://www.mtcr.info/en>]

Restricts export of missile and drone technology.

Founded in 1987. 35 members, not a treaty, but a voluntary informal political understanding among states.

Distinguishes between two categories:

- *Category I* includes rocket and unmanned aerial vehicle systems with a payload of 500 kg and above and a range of at least 300 km. Regardless of export purpose: 'strong presumption of denial'.
- *Category II* includes rocket and unmanned aerial vehicle systems with a payload of below 500 kg and a range of at least 300 km. Subject to strict licensing requirements.

Since 2020, however, the US has decided to treat UAVs with a maximum speed of less than 800 km/hr as Category II, even if all other characteristics place them in Category I. The aim of this policy change is, among other things, to 'increase trade opportunities for US companies', to 'strengthen bilateral relationships' or to 'bolster partner security and counterterrorism capabilities'.[7]

INSTITUTION

Missile Technology Control Regime

Established 16 April 1987 35 Members

The Missile Technology Control Regime (MTCR) is a multilateral, voluntary partnership to prevent the proliferation of missile and unmanned aerial vehicle (UAV) technology capable of delivering weapons of mass destruction (WMD). It focuses on controlling exports of missiles, equipment, software, and technology for missiles.

Arms Trade Treaty (ATT)

Arms Trade Treaty

[<https://thearmstradetreaty.org/>].

Regulates international trade of certain conventional arms.

Entered into force in 2014. 113 State Parties, 28 Signatories that are not yet State Parties, 54 states that have not joined.

Covers eight categories of weapons systems, including battle tanks, armoured combat vehicles, combat aircraft, attack helicopters and warships.

TREATY





Arms Trade Treaty

Effective 02 April 2013 116 Member States

The Arms Trade Treaty regulates the international trade in conventional arms and aims to prevent illicit trading and diversions.

Current Adoption

		MWI	COL	ALB	AND	ATG	ARG	AUS	AUT	BHS	BRB
BEL	BLZ	BEN	BTH	BRA	BGR	BFA	CPV	CMR	TCD	CHL	CRI
CIV	HRV	CYP	CZE	DMA	DOM	SLV	FIN	FRA	GEO	DEU	GHA
GRC	GRD	GTM	GIN	GNB	GUY	HND	HUN	ISL	IRL	ITA	JAM
LVA	LBN	LSO	LBR	LIE	LTU	LUX	MDG	MWI	MLI	MLT	MRT
MEX	MNE	MOZ	NAM	NZL	NER	NGA	MKD	NOR	PLW	PAN	PRY
PER	PHL	POL	PRT	KOR	MDA	ROU	KNA	LCA	VCT	WSM	SMR
STP	SEN	SRB	SYC	SLE	SVK	SVN	ZAF	ESP	SUR	SWE	CHE
TGO	TTO	TUV	GBR	URY	ZMB	AFG	GMB	BWA	CAN	CAF	CHN
GMB	KAZ	MDV	MUS	MCO	NIU	PSE	GAB	JPN	NLD	AGO	BHR
BGD	BDI	KHM	COL	COM	COG	DJI	SWZ	HTI	ISR	KIR	LBY
MYS	MNG	NRU	RWA	SGP	THA	TUR	UKR	ARE	TZA	USA	VUT
ZWE	ARM	AZE	BLR	BOL	BRN	BTN	COD	COK	CUB	DZA	ECU
EGY	ERI	ETH	FJI	FSM	GNQ	IDN	IND	IRN	IRQ	JOR	KEN
KGZ	KWT	LAO	LKA	MAR	MHL	MMR	NIC	NPL	OMN	PAK	PNG
PRK	QAT	RUS	SAU	SDN	SLB	SOM	SSD	SYR	TJK	TKM	TLS
TON	TUN	UGA	UZB	VAT	VEN	VNM	YEM				

-  Adopted by ratification
-  Adopted by accession, acceptance, or succession
-  Signed but not adopted
-  Not adopted

Data: United Nations Treaty Collection

Wassenaar Arrangement

Wassenaar Arrangement

[<https://www.wassenaar.org/>] Entered into force in 1996. Voluntary arrangement comprising 42 states.

Aim: 'to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations'. 'Participating States apply export controls to all items set forth in the List of Dual-Use Goods and Technologies and the Munitions List, with the objective of preventing unauthorized transfers or re-transfers of those items.' Specific UAVs or relevant technologies are controlled in the Arrangements Dual Use List, Category 9.

INSTITUTION

Wassenaar Arrangement

Established 12 July 1996 42 Members

The Wassenaar Arrangement is a multilateral export control regime established on July 12, 1996, in Wassenaar, Netherlands. It aims to promote transparency and responsibility in transfers of conventional arms and dual-use goods and technologies, thereby preventing destabilizing accumulations. Participating states implement national policies to ensure that such transfers do not contribute to the development or enhancement of military capabilities that undermine regional and international security. The Arrangement facilitates information exchange on transfers and denials of specified controlled items to non-participating states, enhancing cooperation among members. It is not legally binding and decisions are made by consensus. The Wassenaar Arrangement's Secretariat is located in Vienna, Austria.

Intermediate-Range Nuclear Forces Treaty (INF) Treaty

Treaty on Elimination of Intermediate-Range and Shorter-Range Missiles between the US and USSR (INF Treaty). Entered into Force 1988.

Eliminated all intermediate-range ballistic missiles with a range between 500 and 5,500 km.

Ceased to be in force in 2019 after US withdrawal over alleged Russian violations.

There was a debate on whether long-range UAVs, such as US Raptors, should be covered by the treaty.

While the Russian position was that they should, the US position – in contrast to the MTCR understanding – made a clear distinction between UAVs and missiles and rejected the Russian interpretation.

TREATY

Intermediate-Range Nuclear Forces Treaty (INF)

Effective 08 December 1987 Ended 2 Member States

The Intermediate-Range Nuclear Forces (INF) Treaty was a landmark arms control agreement signed by the United States and the Soviet Union on December 8, 1987. It aimed to eliminate both nations' land-based missiles with ranges between 500 and 5,500 kilometers. The treaty resulted in the destruction of 2,692 missiles and included extensive verification measures, fostering trust during the Cold War. However, the treaty faced challenges due to alleged violations, leading to the U.S.'s withdrawal in 2019. Despite its termination, the INF Treaty set a precedent for arms control negotiations and efforts to limit the proliferation of nuclear-capable missile systems.

Current Adoption

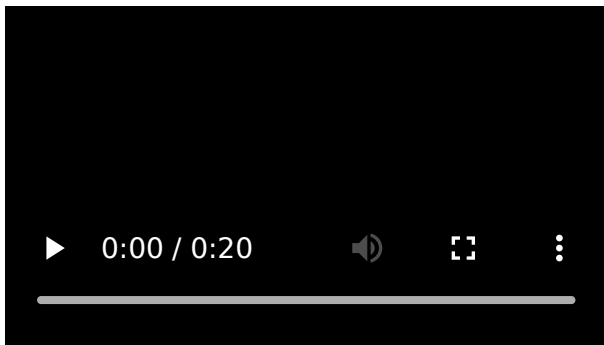
	AFG	AGO	ALB	AND	ARE	ARG	ARM	ATG	AUS	AUT	
AZE	BDI	BEL	BEN	BFA	BGD	BGR	BHR	BHS	BIH	BLR	BLZ
BOL	BRA	BRB	BRN	BTN	BWA	CAF	CAN	CHE	CHL	CHN	CIV
CMR	COD	COG	COK	COL	COM	CPV	CRI	CUB	CYP	CZE	DEU
DJI	DMA	DNK	DOM	DZA	ECU	EGY	ERI	ESP	EST	ETH	FIN
FJI	FRA	FSM	GAB	GBR	GEO	GHA	GIN	GMB	GNB	GNQ	GRC
GRD	GTM	GUY	HND	HRV	HTI	HUN	IDN	IND	IRL	IRN	IRQ
ISL	ISR	ITA	JAM	JOR	JPN	KAZ	KEN	KGZ	KHM	KIR	KNA
KOR	KWT	LAO	LBN	LBR	LBV	LCA	LIE	LKA	LSO	LTU	LUX
LVA	MAR	MCO	MDA	MDG	MDV	MEX	MHL	MKD	MLI	MLT	MMR
MNE	MNG	MOZ	MRT	MUS	MWI	MYS	NAM	NER	NGA	NIC	NIU
NLD	NOR	NPL	NRU	NZL	OMN	PAK	PAN	PER	PHL	PLW	PNG
POL	PRK	PRT	PRY	PSE	QAT	ROU	RWA	SAU	SDN	SEN	SGP
SLB	SLE	SLV	SMR	SOM	SRB	SSD	STP	SUR	SVK	SVN	SWE
SWZ	SYC	SYR	TCO	TGO	THA	TJK	TKM	TLS	TON	TTO	TUN
TUR	TUV	TZA	UGA	UKR	URY	UZB	VAT	VCT	VEN	VNM	VUT
WSM	YEM	ZAF	ZMB	ZWE							

■ Not adopted

Data: United Nations Treaty Collection

Limitations of remotely controlled systems

Despite the military advantages remotely piloted systems offer, these systems require near-constant control and communication links. This renders the vehicle susceptible to discovery or electronic warfare countermeasures. Moreover, latency – that is, the time the control signal needs to travel (sometimes to a satellite in space and back) and get processed – becomes an issue. Depending on the distances involved, this latency can amount to seconds. On top of this is the time the human operator needs to process the information, make a decision and send the respective command back to the vehicle. These additional seconds or minutes can mean the difference between hitting a target or not, winning an engagement or losing the asset.



Daisy-chained line-of-sight connections allow for control and communication without necessarily revealing a system's location, while enabling that system to continue a mission even in operational environments where electronic warfare measures are degrading or disrupting communications. But getting rid of the link entirely would provide even stronger protection against communications disruption or hijacking. This is one of the drivers behind making

uncrewed systems 'autonomous'. The main motive, however, is that removing the uplink and the human from the loop eliminates the invariable delay between the human operator's command and the system's response, thus generating a clear tactical advantage over any remotely controlled and thus invariably 'slower' adversarial system.

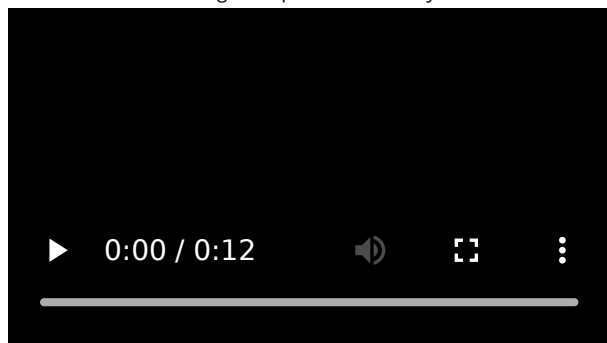
1. Sauer, Frank/Schörnig, Niklas. 2012. "Killer Drones - The Silver Bullet of Democratic Warfare?", in: Security Dialogue 43 (4): 363-80.
2. [<https://www.newamerica.org/international-security/reports/world-drones/>], last updated 30 July 2020.
3. [<https://dronewars.net/who-has-armed-drones/>]
4. Based on [<https://dronewars.net/who-has-armed-drones/#TableB>] and [<https://www.newamerica.org/future-security/reports/world-drones/who-has-what-countries-that-have-conducted-drone-strikes/>]. Other cases where the use is not clearly documented are Saudi Arabia (2015), Egypt (2016) and Somalia (2022). Uses by non-state actors have not been included.
5. Schörnig, N. (2017). Preserve Past Achievements! Why Drones Should Stay within the Missile Technology Control Regime (for the Time Being). PRIF Report No. 149. Frankfurt, PRIF.
6. [<https://www.armscontrol.org/act/2020-09/news/us-reinterprets-mtcr-rules>]
7. [<https://2017-2021.state.gov/u-s-policy-on-the-export-of-unmanned-aerial-systems-2/>]

3. Autonomy in weapons systems

'Autonomy in weapons systems' – a primer

There used to be confusion regarding the proper conceptualisation of weapon autonomy. Is this about 'killer robots'? Does it involve 'lethal autonomous weapons systems', as the UN terminology suggests? Since then research has demonstrated that both in terms of conceptual clarity and regulation, the issue is best understood not as the emergence of a new weapons category but as a shift in human-machine interaction. Hence the proper analytical approach is to take a functionalist perspective, acknowledging that machines rather than humans sometimes perform certain functions during a system's operation and the completion of what is referred to as the 'targeting cycle'.

This includes finding, fixing and tracking the target. Many weapons systems already execute these functions without human input or supervision – for example by navigating via GPS, thus performing the 'finding' function autonomously. Tracking can also be assisted by computer vision systems, making visible what the human eye would have a harder time spotting. A weapon with autonomy, including in the targeting cycle's so-called 'critical functions', executes the final stages of selecting and engaging the target. The tactical advantage of completing the entire targeting cycle at machine speed is the main military rationale for seeking weapon autonomy.



Find

This phase involves identifying potential targets using various intelligence sources, such as surveillance, reconnaissance, or other sensor data. Depending on the context, it also involves moving into the area of

operations. Patterns, movements, and signatures are analyzed to detect threats or mission-relevant targets.

Fix

Once a potential target is identified, efforts focus on precisely locating and confirming its position and distinguishing it from other potential targets as well as civilian infrastructure or personnel. This may include cross-referencing intelligence from multiple sources.

Track

After fixing the target, continuous monitoring begins to maintain situational awareness. This phase ensures the target remains in sight and assesses its movement, behavior, and potential changes in threat level.

Select

Decision-makers evaluate whether the target should be engaged based on rules of engagement (ROE), collateral damage assessments, and mission objectives. This step includes selecting the appropriate weapon system or platform for engagement.

Engage

The final phase involves executing the engagement, neutralizing or destroying the target as per mission requirements. Post-engagement analysis follows to confirm effects and assess any necessary follow-up actions.

But since this is also where thorny ethical, legal and security issues come into play, weapon autonomy is best understood – and defined – as the selection and engagement of targets without human intervention. Note that attempting to delineate autonomy from automation is unnecessary. The terms can be used interchangeably. The crux of the matter is not whether a system is considered automatic or autonomous, but what targets it attacks and under what circumstances. After all, autonomy/automation in the critical functions of weapons systems is not new. It predates the weapon autonomy debate and what we now call AI. Weapon autonomy is also not necessarily problematic, as it can be used – and indeed has been for decades – for defeating incoming munitions to save lives.



Defensive system Phalanx aboard USS Jason Dunham
Paraxade/Wiki Commons/ CC0 1.0 Universal

The key question regarding weapon autonomy is thus not how to define a new weapon category, but who or what – human or machine – is performing the critical functions of the targeting cycle, depending on the operational context, that is, against whom or what, where and when force is being used. Without sound answers to this question – without regulating the application of weapon autonomy in a way that ensures meaningful human control over the use of force – the military advantages could be outweighed by the risky legal, ethical and security implications of weapon autonomy[1]

Ground: Type-X UGV



Type-X UGV.
Milrem Robotics, CC BY-SA 4.0

Type-X is an in-development 12-tonne class unmanned ground vehicle (UGV) made by the Estonian manufacturer Milrem Robotics. Its modular design allows it to carry various weapons systems, such as

autocannons, mortars, anti-tank missiles and more. Its 'Follow me' mode allows autonomous movement, shifting the first step of the targeting cycle from human to machine.

Air: X-47B



X-47B
US Department of Defense.

The US Navy's X-47B was a technology demonstrator run within the Unmanned Carrier-Launched Airborne Surveillance and Strike (UCLASS) system development programme in the early 2010s. The stealthy, subsonic, carrier-based drone demonstrated autonomous take-off and landing as well as mid-air refueling. This testbed was unarmed. Its successor, the MQ-25 Stingray, is a refuelling as well as intelligence, surveillance and reconnaissance platform. Future systems might have strike capabilities.

Sea: CARACaS



CARACaS
US Navy photo by Mass Communication Specialist 2nd Class John Paul Kotar.

CARACaS – which is short for Control Architecture for Robotic Agent Command Sensing – is a module that provides command, control and sensing capabilities to turn a regular (armed) boat into a remotely piloted sea vehicle. When deployed as a swarm, armed CARACaS-controlled boats can autonomously coordinate their behaviour to patrol an area or even defend a convoy against attackers.

Arriving at a multilateral consensus on new binding international law regarding autonomy in weapons systems is difficult, mostly due to the enormous military significance ascribed to the issue. This pertains to consensus between the five permanent members of the UN Security Council, but also to other countries with technologically advanced militaries such as, to name just three examples, Israel, Japan and Australia. This hurdle itself is not new, of course. It is something that was observed in other regulatory processes in the recent past, such as those on landmines, cluster munitions and blinding laser weapons, with the latter being achieved within the framework of the United Nations in Geneva. That said, blinding lasers always represented an exotic niche capability that states could forego at no perceived significant military cost. Landmines and cluster munitions, too, had specific fields of use and were dispensable or at least partly substitutable in the eyes of many states. This is not the case with weapon autonomy. Its impact is perceived to be game-changing for militaries around the globe, comparable to the transition from the horse to the internal combustion engine, and sometimes even mentioned in the same breath as gunpowder and nuclear weapons.

Legal, ethical and security implications of autonomy in weapons systems

Legal implications

A reliable autonomous completion of the targeting cycle that is compliant with the obligations of international humanitarian law (IHL) is not yet feasible from a technological point of view. Few if any representatives of the relevant technical fields believe it to be currently possible for a machine to reliably discriminate between legal and non-legal targets (e.g. between combatants and civilians – which can be extremely difficult, even for humans, because it depends on context and an understanding of social meaning) and make assessments as to the appropriateness of using military means. Moreover, pattern recognition systems based on deep neural networks, which represent the current state-of-the-art in the field of automated image recognition, have proved to be extremely susceptible to manipulation.^[2]

There is considerable legal debate concerning weapon autonomy. Since errors due to software and hardware or the fog of war as well as enemy influence are unavoidable, Lethal Autonomous Weapons Systems (LAWS) carry the risk of causing undue harm for civilians and creating an unacceptable ‘responsibility gap’ in the event of IHL violations. And since the current body of law addresses humans, prompting them to make decisions, simply delegating these same decisions to machines, which are not subjects under the law, seems improper – and makes the creation of new law a prerequisite.^[3]

Ethical Implications

Some researchers contend that viewing weapon autonomy solely through the lens of IHL misses the key point – namely that the delegation of kill decisions infringes on a more fundamental norm: human dignity. The narrow focus on discrimination implies that, as long as civilians remain unharmed, attacking combatants using algorithms could be acceptable. But combatants, too, are imbued with human dignity – and being killed by a mindless machine that is not a moral agent is infringing on that dignity. Algorithmic targeting of humans reduces them to data points and strips them of their right to be recognised as fellow human beings when they are wounded or killed. This matters, especially from a wider societal point of view, because modern warfare, particularly in democracies, is already decoupling societies from war in terms of political and financial costs. A society that also outsources moral costs by no longer even concerning itself with the act of killing, with no individual combatant burdened by the accompanying responsibility, risks losing touch with not only democratic norms but fundamental humanitarian norms as well.^[4]

Security Implications

A strategically relevant implication of machines completing the targeting cycle autonomously is that it might become impossible for humans to intervene as a circuit breaker if operations at machine speed go awry. Weapon autonomy runs the risk of unpredictable outcomes, with a real possibility of swift and unwanted escalations from crisis to war, or, within existing armed conflicts, to higher levels of violence. This risk of ‘flash wars’ is perceived as the biggest incentive for regulation in many countries around the world. This risk is not a problem way off in the distant future. At the Dubai Airshow in 2019, the then chief of staff of the US Air Force, General David Goldfein, presented the simulated engagement of an enemy navy vessel with a next-to-fully automated kill chain. The vessel was first picked up by a satellite, then target data was relayed to airborne surveillance as well as command and control assets. A US Navy destroyer was then tasked with firing a missile, the only point at which this targeting cycle now involved a human decision, with the rest of the ‘kill chain ... completed machine to machine, at the speed of light’.^[5]

The Arms Control Debate at the United Nations

Awareness regarding the implications of weapon autonomy started in expert circles and developed into a fixed field of research in the 2000s. An important milestone in achieving wider recognition of the subject was the formation of the International Committee for Robot Arms Control (ICRAC)

[<https://www.icrac.net/>] in 2009 and its first international conference in Berlin in 2010



Group photo of the participants at the first ICRAC conference, October 2010
Courtesy of ICRAC

The ICRAC is a global network of scholars (of which Frank Sauer has been a member since 2010) working on the topic from the vantage point of their various disciplines. In 2012, the United States' Department of Defense presented the first doctrine on autonomy in weapons systems, lending additional credibility to the issue but at the same time also drawing criticism.

Prompted by ICRAC and the concerns voiced by the scientific community, the non-governmental organisation (NGO) Human Rights Watch, a key player in past humanitarian disarmament processes, began forming a global civil society coalition of NGOs – the Campaign to Stop Killer Robots. Its first goal was to get the issue on and further up the arms control and disarmament agenda of the UN in Geneva. It succeeded in doing so with extraordinary swiftness in 2014, and the Convention on Certain Conventional Weapons (CCW) became the diplomatic and scholarly focal point of the global discussion surrounding autonomy in weapons systems.

The issue of weapon autonomy has now been discussed at the CCW for more than ten years under the rubric of 'Lethal Autonomous Weapons Systems' (LAWS). It should be noted that the term 'LAWS' is problematic. After all, neither 'lethality' nor 'autonomy' are decisive factors in the debate. The military application of non-lethal force raises concerns as well (take the prohibition of blinding lasers as just one example), and the term 'autonomy', philosophically speaking, inappropriately anthropomorphises machines that have limited agency and are incapable of reasoning and reflecting, let alone taking on responsibility. The term 'automation' could just as well be used to describe what is happening, namely the delegation of critical functions from humans to machines. This is what the focus should be on, irrespective of the semantic battles still being fought around the issue.



Informal expert meeting on LAWS at the CCW 2016.
Frank Sauer

Luckily, the functional understanding introduced above has gained considerable traction at the UN level. It has been adopted by the United States in their doctrine, the International Committee of the Red Cross (ICRC) in its position papers and by a majority of civil society organisations, scholars and diplomats. Generally speaking, we are slowly but surely seeing more evidence of convergence in diplomatic talks, resulting in much less 'talking past each other' with regard to the regulatory challenge and how to address it. Convergence is also observable regarding the contours of a potential regulation. A two-tiered approach combining prohibitions and regulations is being discussed by many as a promising structure.

One, specific applications of weapon autonomy are unacceptable to many members of the international community and would thus be prohibited. The ICRC and numerous states suggest that this pertains to all weapons with human target profiles as well as those with potentially unforeseeable or indiscriminate effects on the battlefield due to them being uncontrollable.

Two, autonomous application of force against target profiles other than those intended to represent humans, such as various military objects, is acceptable but requires certain limits and constraints, that is, positive obligations to minimise ethical risks, ensure compliance with IHL and address security and safety concerns. Those limits and constraints can be temporal or spatial and are generally speaking subsumed under the notion that 'meaningful human control' must be preserved in the design of a weapons system, along with adequate tactics, techniques and procedures for use.

It is however crucial to state that there is no such thing as 'one-size-fits-all meaningful human control'. Operationalising human control is a case-by-case process. Human control also has to be 'baked into' the system at the design stage. Hence, understanding the human element as human control both 'by design' and 'in use' means that a need to differentiate arises. On the one hand, defending against lifeless incoming munitions remains one application of autonomy that can rely on a weapon's critical functions being performed without human intervention, provided that decision is delegated to a machine set up with the spatial and temporal limits that are appropriate in the

operational context. On the other hand, selecting and engaging targets in a cluttered environment at points in time that are hard to ascertain in advance requires much greater human judgment and agency. In other words, in this case humans have to decide with what, when and where to engage, particularly when an application of military force could endanger human life.

In sum, while the conceptual struggles around weapon autonomy are less of a pressing concern nowadays, the struggle to muster the political will to enact regulation at the UN level is still ongoing.

1. Sauer, Frank. 2021. "Stepping back from the brink: Why multilateral

regulation of autonomy in weapons systems is difficult, yet imperative and feasible", in: *International Review of the Red Cross* 102 (913): 235–59.

2. Sauer, Frank. 2022. "The military rationale for AI", in: Schörnig, Niklas/Reinhold, Thomas (eds): *Armament, Arms Control and Artificial Intelligence: The Impact of Software, Machine Learning and Artificial Intelligence on Armament and Arms Control*, 27–38.
3. International Committee of the Red Cross 2021: ICRC position on autonomous weapons systems, Geneva.
4. Rosert, Elvira/Sauer, Frank. 2019. "Prohibiting Autonomous Weapons: Put Human Dignity First", in: *Global Policy* 10 (3): 370–75.
5. Video: 'Here's How the US Air Force Is Automating the Future Kill Chain', *Defense News*, 2019, available at: [<https://www.defensenews.com/video/2019/11/16/heres-how-the-us-air-force-is-automating-the-future-kill-chain-dubai-airshow-2019/>].

4. Artificial intelligence and quantum computing

Artificial intelligence

Milestones of the last 20 years and recent military applications

Artificial Intelligence (AI) is the future. [...] Whoever leads in AI will rule the world.

Vladimir Putin, Sept. 1, 2017

This was the central message that President Vladimir Putin conveyed to more than one million Russian school pupils in a video call in September 2017. The announcement was no surprise: AI has become one of the most promising technologies in more recent history and the pace of progress is astounding – this holds true both for the civilian and the military realm.

Most people forget, for example, that as late as 2004, autonomous cars were unable to drive more than a couple of miles on an empty desert track. In 2005, however, five cars were able to finish the second DARPA Grand Challenge, a race for robotic cars funded by the US Defense Advanced Research Projects Agency (DARPA).

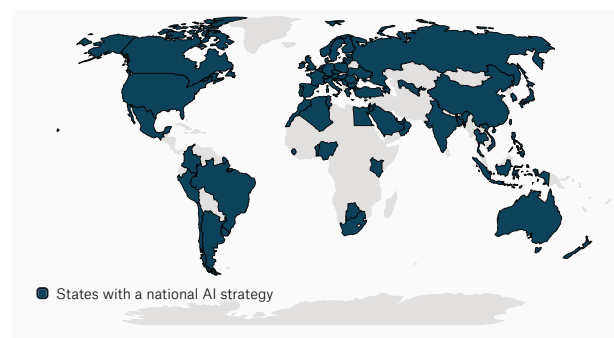


'Stanley': Winner of the DARPA Grand Challenge 2005 in the Smithsonian National Air and Space Museum, Washington, D.C., 2015.
Niklas Schörnig

While we are not seeing fully autonomous cars mixing with human-steered vehicles just yet, many AI-based technologies and assistant systems have already found their way into commercial current generation vehicles. Artificial intelligence has also surpassed human capabilities in contexts where many observers were expecting human superiority for a long time to come. 1996 the computer-program Deep Blue had beaten the Chess World Maser Kasparov with a simple brute-force approach.

In 2016, Google's AlphaGo Program beat Grandmaster Lee Sedol in Go, a game significantly more complex than chess.

Another milestone was reached in August 2020. Again this was down to DARPA, pitching an AI-controlled jet fighter against a human Air Force pilot in a simulated dogfight. While the conditions were not as symmetric as in Go, the fact that AI won five to nil against the human was seen as the start of a new era by many. When it comes to the use of AI, the United States and Russia are not the only countries with a strategic interest in what artificial intelligence has to offer. Many countries have published AI strategies for the coming years and decades.[1]



States with a national AI strategy
Data: Natural Earth. Graphic: PRIF
Licensed under CC BY 4.0.

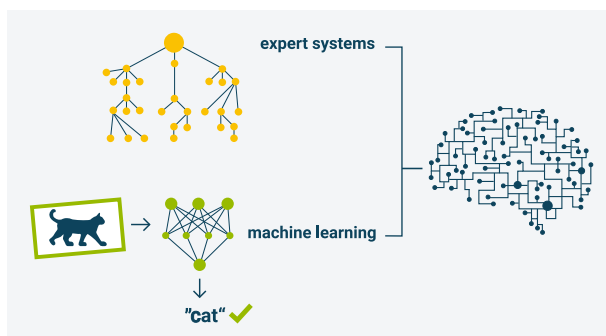
It is no wonder that militaries worldwide are keen to implement AI to enhance their capabilities.[2] The number of military applications for AI are vast:

- Analysis of data collected by all kinds of sensors on the battlefield
- Identification and classification of potential targets, even camouflaged
- Enhanced automation of drones or the control of drone swarms
- Support of tactical decisions, or even optimised logistics

What is obvious from this list is that AI is widely perceived not as a particular weapons system but as an enabler – just as the combustion engine was at the beginning of the 20th century. With the US, Russia, China – and to some extent the EU – competing for AI leadership, the fear of an AI arms race does not seem too far-fetched. In any case, the use of AI in the military realm is going to increase significantly in the years to come.

Artificial intelligence: What it is and how arms control can benefit from it

While most people think they know what AI is, it is always important to clarify what is understood by the term 'AI' in a specific context. There are two basic forms of AI. On the one hand, we have very complex 'expert systems', which can be understood as tremendously complex decision trees, where the system 'decides' based on a high number of different variables. In principle, these systems are deterministic as the same starting conditions always lead to the same result. Yet, due to the sheer complexity and number of variables, humans do have difficulty keeping up. While these systems were very common a few decades ago, modern systems use a different approach.



Expert system vs neural net
Grüebelfabrik, CC BY-NC-SA

What are more common today are AI systems based on machine learning. Here the system compares large amounts of data for similarities using statistical models. Given enough pictures of, for example, cats, the system can use statistical methods to determine similarities to identify cats on new pictures without being told what to look at. Machine learning has made tremendous progress in the last couple of years and some experts today only use the term AI to refer to machine learning algorithms. Another form of AI is "deep learning", where the computer learns by trying to replicate a neural net as in the human brain.

But machine learning AI is not without difficulties. Expert Gary Marcus, for example, came up with four characteristics of AI^[3]. Its 'greedy' (that is hungry for data), 'brittle' (fails spectacularly when confronted with untrained tasks), 'opaque' (prone to inexplicable errors and therefore difficult to debug) and 'shallow', because despite the use of the term 'deep learning', there is in fact no understanding of what has been learned.

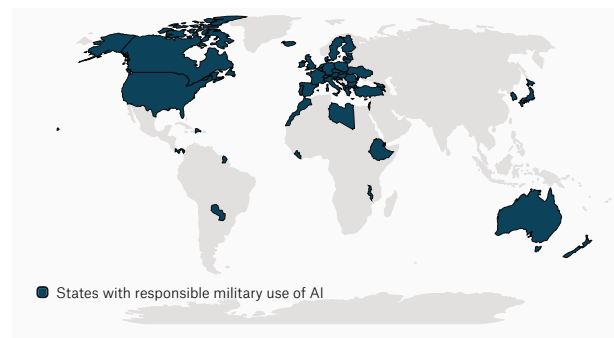
This raises the basic question: How can one be sure about what the algorithms have actually learned? As correlation is not causation, how can AI be 'trusted'?

From a military perspective, the issue of reliability is at least as important as in the civilian sphere. Imagine an AI-powered lethal autonomous weapons system going rogue, maybe even starting a war by mistake. Some experts fear that in a war of necessity, a war where national survival is at stake, states might use untested or unverified military AI to gain superiority.

While this is indeed a potential risk, many states are at least aware of the danger of unrestricted use of unreliable AI and some suggest developing norms on which to base the military use of it.

One of the most important initiatives is the 'Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy

[<https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/>]' – launched in early 2023 by the United States and (as of February 2025) endorsed by 58 states.^[4]



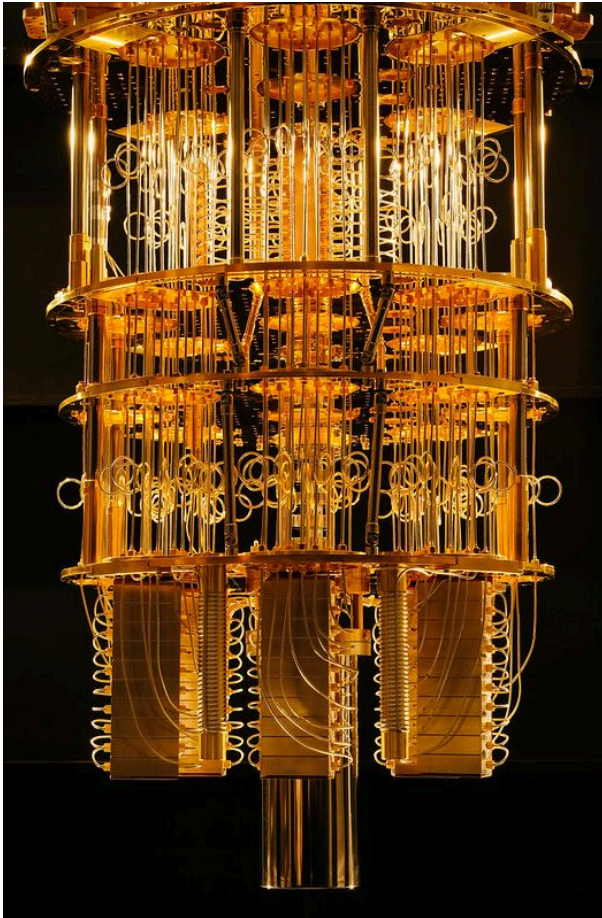
States with responsible military use of AI
Data: Natural Earth. Graphic: PRIF
Licensed under CC BY 4.0.

The declaration features ten measures, including, for example, the call for states to take proactive steps to minimise unintended bias; train users to sufficiently understand the capabilities and limitations of AI-powered systems; ensure that AI capabilities only have explicit, well-defined uses; and implement appropriate safeguards, e.g. the ability to deactivate a system when it shows unintended behaviour.

But an even more profound revolution in computing is in the starting blocks, one that will potentially cause even greater upheaval than machine learning already has. The technology we are talking about here is quantum computing.

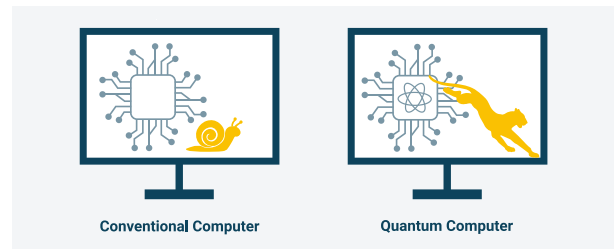
Quantum computing

Quantum computers take the principle of miniaturisation which classical computers have followed down to the single atom on the next lowest level by utilising the fundamentally different physical principles that apply on the sub-atomic level for computer operations.



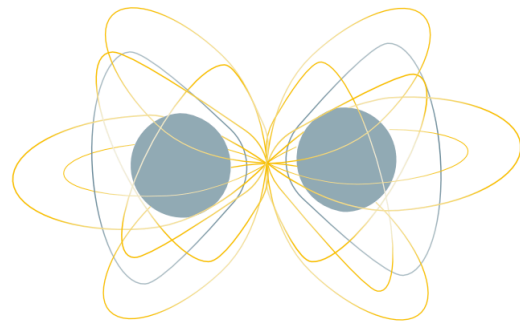
Experimental quantum computer at the IBM Quantum Lab in Yorktown Heights, New York
IBM Research, CC BY-ND 2.0

Superposition is the first such phenomenon used for this purpose. It involves superposing different states. Quantum computers use superposition in quantum bits (qubits), which, unlike classical bits with their two discrete states (1 or 0), can take on all states between 1 and 0 at the same time. Quantum computers thus offer massive parallel computing performance compared with classical computers. They are also better at scaling – at least in theory – because ideally every additional qubit doubles the computer's performance, which thus grows exponentially. With computing tasks of exponentially increasing complexity, quantum computers develop solutions quickly (in seconds or minutes) where even the biggest classical supercomputers would need too much time (tens of thousands of years). This is what is commonly understood by the term 'quantum supremacy'.



Speed advantage through 'quantum supremacy'
Grüebelfabrik, CC BY-NC-SA

The second phenomenon utilised in quantum computing is entanglement. Entanglement means that two or more particles are linked with each other, i.e. they can represent the same state, even over long distances. The numerous possibilities for flexibly manipulating such entangled qubits contribute to the speed with which a quantum computer is able to handle complex computing problems.



Quantum Entanglement
Grüebelfabrik, CC BY-NC-SA

There are still a number of difficult hurdles to overcome before quantum computing can be used on a widespread basis (by miniaturising mass-producible architectures). Sceptics note that quantum computers could face the same fate as atomic fusion. Decade after decade, it has been predicted that this technology will finally have its breakthrough. But this breakthrough never seems to materialise.

However, if quantum computers were to one day make their way out of the lab and into everyday applications, the implications would be extremely wide-ranging. From a military perspective, the most important elements to focus on would be quantum cryptography and quantum sensing.

Quantum cryptography

When it comes to cryptography, established cryptographic methods take advantage of the fact that certain mathematical problems cannot be solved in a reasonable time frame by classical computers. As outlined above, quantum computers have the potential to introduce a paradigm shift in this respect by very quickly decrypting databases that, by current standards, have been securely encrypted. Stored

datasets that so far have been impossible to decipher could also suddenly be accessed.

At the moment, this is just a theoretical scenario. Nevertheless, ideas for quantum computer-resistant encryption methods for the world of classical computers and the internet are already being discussed. In 2016, for example, the National Institute for Standards and Technology (NIST) in the US already initiated a process to develop and standardise such methods and make them more readily available. The first results for such quantum computer-resistant encryptions are currently under review.

In light of the progress that has been made in just under three decades, the prototypes and special applications that already exist, the investments already made and, last but not least, all the talent and time that has been devoted to the field worldwide, when it comes to a quantum computing breakthrough, it is more likely a question of 'when' rather than 'if'.

Quantum sensing

Sensor technology is the area of quantum technology with the highest number of concrete applications that are already in use. Unlike quantum computers, quantum sensors do not require large numbers of entangled pairs of particles. Considerable advances over the last two decades when it comes to the production and manipulation of the quantum states of

particles also mean that research now has a better handle on 'noise', which of course affects the precision of measurements. Much like in the field of computers, a variety of different physical principles and designs are also being explored simultaneously.

With quantum sensors, mass, time, place, speed, acceleration and electromagnetic field strength can be measured several orders of magnitude more accurately than with classical sensors. Spatial resolutions in the nanometre range are possible. Quantum clocks make it possible to synchronise processes precisely. Quantum gyroscopes for inertial navigation systems and quantum sensors for measuring earth's magnetic field can make autonomous mobility possible without having to rely on GPS or other satellite navigation systems. Compact quantum magnetometers that work at room temperature are currently being developed. These could be used in areas ranging from submarine detection to brain-computer interfaces.

1. Galindo, L./ Perset K./ Sheeka, F. 2021. "An overview of national AI strategies and policies", in: OECD Going Digital Toolkit Notes, no. 14, OECD Publishing, Paris, available at: [<https://doi.org/10.1787/c05140d9-en>].
2. Sauer, Frank. 2022. "The Military Rationale for AI", In: Reinhold, T./Schörnig, N.: Armament, Arms Control and Artificial Intelligence. The Janus-faced Nature of Machine Learning in the Military Realm. Springer, 27–38.
3. Marcus 2018: [<https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf>]
4. [<https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/>]

5. 3D printing, Nanotechnology and Human Enhancement

3D printing

Additive manufacturing, more commonly known as 3D printing, is about to transform the way we make things. In contrast to traditional manufacturing, 3D printers build objects from digital build files by depositing and joining successive layers of material. 3D printers can process a wide variety of materials, including plastics, metals (such as steel or aluminum), ceramics and even organic tissues. Many industries, with the automotive, aerospace and healthcare industries at the forefront, already draw on 3D printing – not only for rapid prototyping but more and more also for the production of end-use parts. Additive manufacturing offers many advantages over traditional manufacturing. It makes it possible, for example, to produce parts with complex geometries, such as lattices or hollow structures, which could not be produced by traditional molting techniques. The resulting parts are lighter, yet stronger. Additive manufacturing is a potentially disrupting technology that brings not only benefits but also risks, in particular for (international) security. Military planners and defence contractors have already realised the potential of additive manufacturing – but so have non-state actors. 3D printed drones and handguns have already proven to be functional and designers have made significant progress over the last couple of years. Compare, for example, the first functioning printed gun, the single shot 'Liberator', developed in 2013 with the most recent submachine-type FGC-9 – with FGC standing for F*** Gun Control.



Prototype of FGC-9.
JStark1809/Wikimedia, CC-BY-4.0

While the printing and possession of these weapons is of course illegal, police raids have already discovered workshops 'mass' producing printed guns. Obviously, this poses huge challenges for domestic security. While buying regular small arms from the diverse

battlefields of the world might still be an easier option than printing firearms, terrorists could use 3D printing, for example, to produce ceramic or plastic firearms that could pass unnoticed through metal detectors. Or they could 'print' a swarm of cheap drones, equipped with C-4 plastic explosives to be used as improvised explosive devices.

3D printing may also impact on the proliferation of weapons of mass destruction (WMD). While we are a long way from having to worry about someone being able to '3D print the bomb'^[1], additive manufacturing may facilitate clandestine state and non-state WMD programmes. Proliferators could, for example, use the technology to illicitly manufacture components of a gas centrifuge at less risk of being exposed.

The good news, at least for the moment, is that most technicians agree that printing weapons still requires a lot of manual craftsmanship and skill when it comes to the finishing of the product. But this might change in the future.

Human enhancement

What is 'human enhancement'?

According to a 2021 report by the UK Ministry of Defence and the Bundeswehr Office for Defence Planning,

'[t]he paradox of war is that humans are central to its conduct but are also the weakest link'.^[2]

However, the idea of enhancing a warfighter's quality by either using tools – weapons or armour – or drugs is almost as old as warfare itself. And injured or maimed soldiers have long been given prostheses and artificial limbs to help them regain some quality of life. For a very long time, however, these 'enhancers' were inferior, not very practical or even dangerous. Almost all drugs do have negative side effects, including addiction. Body armour was heavy and restricted movement. And replacements for limbs were ungainly and crude. What is new, however, is the expectation that high-tech solutions can actually enhance human performance without drawbacks. Three ways to enhance the human body are currently heavily researched.

The most 'conventional' approach focusses on active, that is battery-powered equipment attached to the human body. While active night vision goggles have been used by the military for decades now, motor-driven exoskeletons are being tested to enhance a soldier's endurance, strength and resilience.



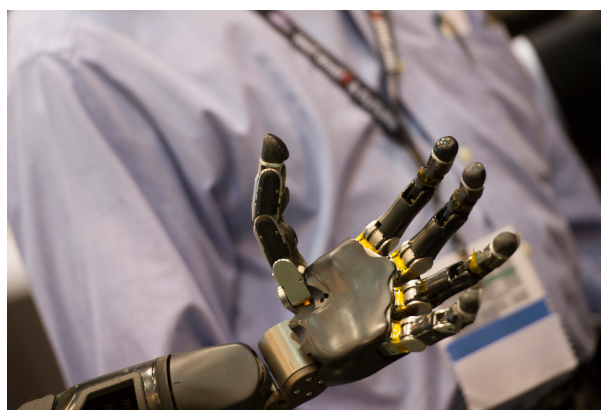
Exoskeleton makes it easier for an American soldier to lift heavy loads – here, for example, an artillery shell. Picture from an exoskeleton Operations and Maneuver and Technology Interchange meeting, 2018. [US Army]

(https://www.army.mil/article/214540/exoskeleton_event_brings_teams_together_to_advance_exoskeleton_technology)

The development of miniaturised motors, tough but lightweight materials and high-capacity power supplies has boosted this development. It is obvious that while these enhancements might improve the individual soldier, the overall impact on a military's fighting power is limited. It is also obvious that the impact on the individual soldier's health is minimal, as these enhancements are fully reversible.

The second field to look at when talking about human enhancement is also an old one: the use of chemical drugs to improve the individual warfighter's ability to fight. Already in ancient times warriors drugged themselves by chewing certain leaves. Drinking coffee as a means to stay awake is common, not only in the military. During World War II, a drug called Pervitin, which is now known by the name 'Meth', was given to German soldiers to stay awake.[3] But one can also bring to mind a broad range of vaccinations used to keep soldiers fit under harsh conditions. New technologies in the biosciences might result in significantly more potent drugs. In contrast to the category debated above, the use of drugs might not be fully reversible and can have lasting impacts by creating life-long addictions.

This might be even more important for another form of human enhancement, sometimes referred to as 'bodyhacking'.[4] The development of new materials and technologies has significantly improved the availability and performance of prostheses and implants in the civilian sector, which were previously only intended for people who had lost real body parts, e.g. through accidents or war.



Robotic hand prosthesis
US DoD/Senior Master Sgt. Adrian Cadiz

Some observers speculate, however, that in the not too distant future, soldiers will or might even be ordered to undergo surgery to have certain parts of their body permanently replaced by enhanced artificial products to improve performance or sensation – the idea of the cyborg becoming reality. While the notion of sacrificing healthy limbs or organs and replacing them with enhanced artificial versions feels rather Cyberpunk and dystopian, the idea of improving humans with (removable) implants seems rather doable in comparison. Human-machine interaction via implanted computer-brain interfaces, for example, does not seem that far off anymore.[5] It is plausible to assume, for instance, that someone with a direct computer-brain interface can control autonomous weapons in a much faster and far more effective fashion than someone relying on a traditional mouse and keyboard – reaping the advantages of autonomous weapons by still providing human control.

The fourth field encompasses the design of new artificial biological or chemical systems with as yet unknown qualities. This is known as 'synthetic biology' and involves changing humans on the most basic level – i.e. that of the genome – with the help of techniques like CRISPR-Cas.

However, at least in areas three and four, military players are currently funding basic research rather than concrete applications (see Learning Unit 03 for more details). However, in 2019, the US military forecast that human enhancement technologies would be widely available by 2050[6].

Legal and ethical implications of human enhancement

As described above, the idea of enhancing ordinary humans to create some sort of super soldier is not new. And some enhancers, whether technological or biochemical, are already in use. However, aside from a slowly expanding scientific discourse, there has been almost no international debate about the implications of current technological developments. These developments raise new legal, ethical and political questions.[7] The first and most obvious question pertains to the risks one is willing to take or ask others

to take. Every medical procedure involves certain risks for those who undergo it. There has, for instance, been a debate on whether a state can order a soldier to get a risky vaccination. Forcing a soldier to accept an implant or even to replace a healthy limb or organ is even more intrusive and fundamental. Negative side effects can never be ruled out. Do soldiers have to accept these risks to become, for example, a member of an elite unit?

Depending on the grade of enhancement a human has undergone: would they still count as humans with the rights of a POW or would they be considered a weapon in and of themselves? Would it be legal to 'deactivate' certain functions of captured soldiers, i.e. 'switch off' their artificial legs?

In addition, what are the risks to others – especially when it comes to stimulants or drugs. Can soldiers be held accountable for war crimes if they were 'high' when they committed them? What if there are unforeseen adverse reactions to other enhancers or medicines?

Another important issue is of ethical nature: Is it ethical to ask soldiers to potentially irreversibly enhance their bodies? Would they have to give back implants or certain abilities once they leave the military? Would that preclude any permanent enhancements?

We do not claim that there are no answers to these questions. Most can probably be answered in a satisfactory way based on existing law. However, up to now there has simply been no international forum where these questions can be raised and addressed, let alone answered.

Nanotechnology

Facts and figures

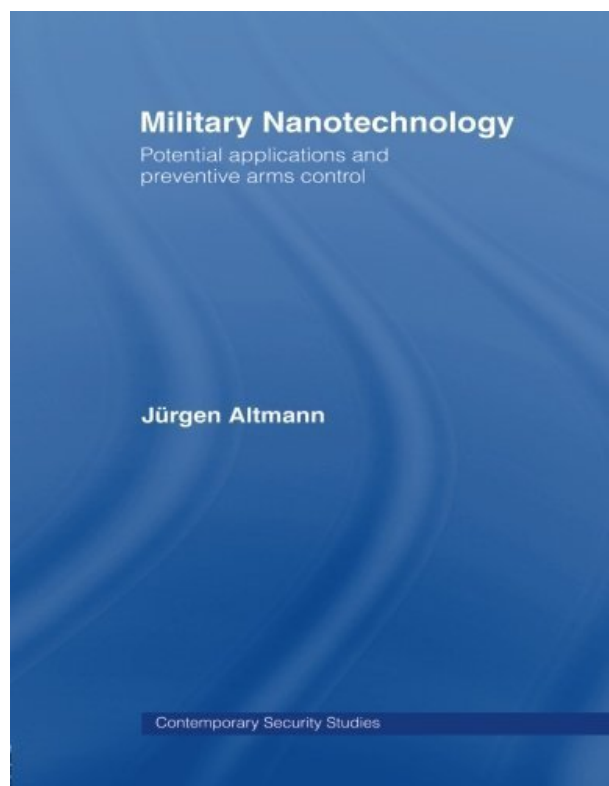
A nanometre (nm) is defined as a millionth of a millimetre – which is approximately the size of a glucose molecule. Nanotechnology (or nanotech) involves creating or manipulating precisely such very small objects on an atomic or molecular scale. When experts use the term nanotech, they are usually referring to systems measuring between 0.1 nm and 100 nm. Nanostructures offer the possibility of creating new materials with enhanced, novel or unique characteristics and capabilities, even including electromechanical objects on a nanoscale. The ultimate goal is to design nanomaterial by placing individual atoms or molecules in a predesignated location in a structure.



Size comparison between nano and macro
Grüebelfabrik, CC BY-NC-SA

Governments started to be really interested in nanotech at the advent of the new millennium. From the very beginning, the USA has been at the forefront of the nanotech revolution, initiating, for example, the National Nanotechnology Initiative (NNI), a federal research and development programme, as early as 2000. Between 2001 and 2023, the NNI received a total of US\$ 40.7 billion^[8] from participating agencies, including – amongst others – the Department of Defense (DOD), Department of Energy and NASA. Its current budget is roughly two billion, with 45 percent of that being spent on foundational research and 35 percent on concrete applications. While the relative share of the DOD's contribution declined after 2013, it has increased again since the beginning of the 2020s. Other countries with a strong interest in nanotech include member states of the European Union (especially Germany and the UK), Japan, China, Russia and Korea. While many nanotech applications are civilian, nanotechnology might have an impact on numerous military-related issues as well. Reducing the weight soldiers have to carry is one likely application, for example by creating lighter but still robust body armour, weapons and equipment. Lighter yet more powerful batteries and computers can facilitate new forms of tactical communication. Nanostructures can also enhance the effectiveness of drugs, explosives or propellants. Some projects based on nanotechnology are working on active optical camouflage for individuals, tanks or even warships. Scholars even envision the development of 'smart dust', made up of a network of communicating sensors smaller than one cubic millimeter.

Experts who have been covering nano since the early 2000s (especially German physicist Jürgen Altmann) saw nanotech, from very early on, as being a perfect candidate for preventive forms of arms control, that is restrictions based on the forecast threat of an emerging technology.



Still the seminal book on military nanotechnology by Jürgen Altmann
Routledge

[9]

However, there has not been any serious attempt to regulate military nanotechnology yet. Some of the reasons for this might be the following:

- First, nanotechnology is a classical dual-use technology. New materials with extraordinary characteristics will find application in the military as well as the civilian sector. Growth of the civilian market is forecast to be in the double digits for years

to come. So, finding a balance between legitimate civilian interests and military restrictions will be hard.

- Second, as the diverse range of potential applications of nanotech demonstrates, it would be counterproductive to try to restrict nanotech per se.
- Third, many military applications of nanotech still look like science fiction to the uninformed observer. While arms control advocates emphasise the precautionary principle, 'invisibility cloaks' (aka 'active camouflage') or smart dust still seem way too far out for many political decision-makers to focus on.

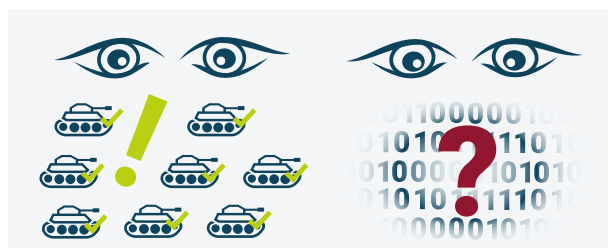
In sum, how to prevent or even stop a potential nanotech 'arms race' is still an open question – and one that is not receiving an awful lot of attention at the moment.

1. Volpe, T./Kroenig, M. 2015. "3-D Printing the Bomb? The Nuclear Nonproliferation Challenge".
[<https://carnegieendowment.org/2015/11/04/3-d-printing-bomb-nuclear-nonproliferation-challenge-pub-61920>]
2. UK MoD 2021: Human Augmentation – The Dawn of a New Paradigm. A strategic implication project.
[https://assets.publishing.service.gov.uk/media/609d23c6e90e07357baa8388/Human_Augmentation_SIP_access2.pdf], p.11.
3. [<https://time.com/5752114/nazi-military-drugs/>]
4. UK MoD 2021: Human Augmentation – The Dawn of a New Paradigm. A strategic implication project.
[https://assets.publishing.service.gov.uk/media/609d23c6e90e07357baa8388/Human_Augmentation_SIP_access2.pdf], p. 60.
5. UK MoD 2021: Human Augmentation – The Dawn of a New Paradigm. A strategic implication project.
[https://assets.publishing.service.gov.uk/media/609d23c6e90e07357baa8388/Human_Augmentation_SIP_access2.pdf], p. 90–1.
6. [<https://apps.dtic.mil/sti/pdfs/AD1083010.pdf>]
7. Lin, P., et al. 2013. "Enhanced Warfighters: Risk, Ethics, and Policy". New York, The Greenwall Foundation; UK MoD 2021: Human Augmentation – The Dawn of a New Paradigm. A strategic implication project.
[https://assets.publishing.service.gov.uk/media/609d23c6e90e07357baa8388/Human_Augmentation_SIP_access2.pdf]; Burt, Peter. 2023. "Cyborg Dawn? The military use of human augmentation for war fighting". Drone Wars UK, [<https://dronewars.net/wp-content/uploads/2023/05/DW-Cyborg-Dawn-WEB.pdf>].
8. [<https://www.nano.gov/2023BudgetSupplement>]
9. Altmann, Jürgen. 2006. Military Nanotechnology. Potential applications and preventive arms control. Routledge

6. Arms control and EDT – new concepts, new opportunities?

From quantitative to qualitative arms control

How can arms control respond to the challenges stemming from this plethora of new technologies? One thing is certain – in most cases the traditional, quantitative-oriented approaches fail. In contrast to tanks or missiles, counting weapons based on new and emerging technologies is a futile exercise.



Classical verification vs. verification of software
Grüebelfabrik, CC BY-NC-SA

Consequently, the key lies in a qualitative rather than a quantitative approach. Take autonomy in weapons systems as an example. From an arms control perspective, the main insight here is that the good old days of treaties and regimes relying mainly on quantification for verification and compliance are over. Dual-use hardware and software is what makes these conventional weapons systems tick. And numbers are less important than capabilities.

Exotic and hard to come by fissile materials and complicated enrichment procedures or chemical precursors and laboratories are not required to build autonomous weapons systems that can wreak havoc on an enemy force or even a civilian population in a terrorist attack; there are no warheads for an inspection team to count, maybe not even facilities or weapons systems to scrutinise in an inspection.

In the not too distant future, the hardware of a weapon with autonomy in target selection and engagement might be 3D-printed just-in-time, and the software running it can be stolen online and enhanced using AI.



Grüebelfabrik, CC BY-NC-SA

Consequently, if regulation – that is, an internationally agreed legal instrument providing guard-rails for the use of weapon autonomy – is desirable, then specific

uses rather than numbers of weapons systems need to be addressed. There is no fixed category of ‘autonomous weapons’ to be clearly delineated from ‘non-autonomous weapons’. Hence the target of regulation cannot be the hardware. Instead, it must be the human-machine relationship. Who or what – human or machine – is deciding what, when, and under what circumstances. This question needs addressing in a context-dependent manner to assure that humans remain meaningfully in control of decision-making and thus legally accountable and morally responsible when deadly military force is applied.

The same holds true for military AI in a broader sense. First, AI is a functionality, instantiated by intangible software code. Second, AI is a dual-use technology, and military AI is based on civilian developments transferred to military applications. Third, AI is not a weapon but a general enabler. A specific AI model might be problematic when applied to a specific weapons system, but entirely benign in other contexts. This will be difficult to address from an arms control perspective. Controlling AI is nevertheless important, as AI has the potential to speed up processes, reduce warning times and thus crisis stability.

So, on a very general level, these new technologies pose a serious challenge for classical arms control thinking, especially when it comes to legally binding treaties with clear verification measures.^[1]

On the other hand, some good ideas for arms control in the realm of EDT have been already pitched.

Using EDT for arms control – new opportunities

While many focus only on the negative effects of emerging technologies in the military, many new technologies also have at least the potential to help with verification and support weapons inspectors. The most obvious case is the use of unmanned systems for measurements or sample collection in hazardous environments which are unsafe for humans. Small systems can access hard-to-reach places and underwater drones can operate in flooded areas. While the use of physical drones or new and more precise sensors has rather obvious advantages, arms control experts are also thinking hard about how AI could make their lives easier. In the area of arms control, AI-based processes can improve verification, i.e. the accuracy and speed at which contract breaches can be identified, and therefore deter potential fraudsters. The spectrum of possible applications ranges from the analysis of trade data to uncover clues on the

proliferation of weapons of mass destruction, to the identification of landmines that is boosted by AI with improved ground-penetrating radars.^[2] Others are experimenting with AI for detecting change within satellite images, e.g. to identify the expansion of bases, the analysis of open source pictures to identify facilities that are in operation, or to support the analysis of seismic occurrences to detect unnatural events like the testing of a nuclear device.^[3] But other possibilities worth considering might be the use of translation software, improving, for example, inspectors' abilities to evaluate and understand large amounts of relevant documents.



US Army/public domain

The idea of using AI as a tool for arms control is not new. In as early as 1987, a volume on 'Arms and Artificial Intelligence', published by SIPRI, dedicated a whole chapter to the issue.^[4] Artificial intelligence has only become more capable since then, and many pilot projects have shown that it can enhance arms control significantly.

Artificial intelligence could bring a new level of objectivity to arms control and reduce human error and bias.

In an internal poll conducted by the IAEA, 86 percent of respondents were either 'very' or 'somewhat confident' 'about the prospect of AI and ML to help the Department in safeguards surveillance' (IAEA 2020, p. 12).

However, since the results of AI models are highly dependent on external factors, especially the data used to train them, the use of AI in arms control raises a new issue: Can the model be 'trusted'? Whether states adhering to an arms control regime are willing to accept analysis based on 'opaque' algorithms remains an open question. Most commentators therefore agree that, while AI can be a useful tool to support arms control, it should be deployed to assist human officials, not replace them.

In sum, it is obvious that arms control can be significantly improved with the use of new emerging technologies, but new technologies probably won't revolutionise arms control. As long as the relevant actors do not trust each other, it is unlikely that new technologies will be able to compensate for that lack of trust.

1. Reinhold, Thomas. 2022. "Arms Control for Artificial Intelligence", In: Reinhold, T./Schörnig, N.: Armament, Arms Control and Artificial Intelligence. The Janus-faced Nature of Machine Learning in the Military Realm. Springer, 211-26.
2. Lück, Nico. 2019. "Machine Learning-powered Artificial Intelligence in Arms Control", PRIF-Report 8/19, [https://www.prif.org/fileadmin/HSFK/hsfk_publicationen/prif0819.pdf]
3. Schörnig, Niklas. 2022. "Artificial Intelligence as an Arms Control Tool: Opportunities and Challenges", In: Reinhold, T./Schörnig, N.: Armament, Arms Control and Artificial Intelligence. The Janus-faced Nature of Machine Learning in the Military Realm. Springer, 57-72.
4. Din, A. M. (ed.). 1987. Arms and Artificial Intelligence. Oxford University Press.

7. The EU and emerging technologies

Given the diverse nature of the issues covered in this learning unit as well as the different stages of technological development, it is hard to summarise the EU's activities with regard to emerging technologies. Some of the issues covered in this unit have not yet led to a systematic and comprehensive review by EU institutions.

Others, however, like drones, AI and LAWS, have received more attention over time. After all, the EU is also interested in quantum technology and nanotechnology, but only for peaceful purposes. Military issues or matters related to preventive arms control are not discussed in these areas. However, this is not surprising, since, as described above, there has been no international discourse on any form of regulation in this area to date. And different actors had different perspectives, of course. The European Parliament (EP) started focusing on drones and drone warfare very early. On 27 February 2014, the EP already adopted Resolution 2014/2567(RSP) [<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014IP0172>] on the use of armed drones, drawing attention to the increase in extraterritorial lethal operations by drones and the resulting civilian death toll, calling

'drone strikes outside a declared war by a state on the territory of another state without the consent of the latter or of the UN Security Council [...] a violation of international law'.

European Parliament resolution of 27 February 2014 on the use of armed drones (2014/2567(RSP))

In contrast, the Commission did not take a position on armed drones or their worldwide use and focused mainly on the civilian use of unmanned systems.

In the LAWS sector, however, the European actors are more in agreement.

Notably, in its 2014 resolution, the EP also called for a 'ban [on] the development, production and use of fully autonomous weapons which enable strikes to be carried out without human intervention'. In 2018, the EP adopted a resolution on autonomous weapons systems (2018/2752(RSP))

[https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html], stressing, inter alia, that

'EU policies and actions are guided by the principles of human rights and respect for human dignity, the principles of the UN Charter and international law; whereas these principles should be applied in order to preserve peace, prevent conflicts and strengthen international security'

European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP))

and that

'human involvement and oversight are central to the lethal decision-making process, since it is humans who remain accountable for decisions concerning life and death.'

European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP))

In 2021, the EO adopted another resolution (2020/2013(INI)), this time with a broader perspective on artificial intelligence and international law, which referred to both civilian and military use, but also directly addressed the issue of LAWS and, as in 2018, emphasised 'the need for an EU-wide strategy against LAWS and a ban on so-called "killer robots"'.

The official representatives of the EU delegation to the United Nations in Geneva did not want to go as far as the EP, but nevertheless emphasised the importance of human controls and the limits set by international law. In 2023 and again in 2024, an EU representative and official participant in the GGE negotiations on LAWS stated[1]

'that human beings must make decisions with regard to the use of force, exert control over weapons systems that they use and remain accountable for decisions over the use of force in order to ensure compliance with International Law, in particular International Humanitarian Law (IHL), taking into account ethical considerations.'

Finally, the EU is also interested in quantum technology and nanotechnology, but only for peaceful purposes. Military issues or questions of preventive arms control are not discussed in these areas. However, this is not surprising since no international discourse on any form of regulation has taken place in this area to date.

Further reading

- Sauer, Frank. 2022. "The military rationale for AI", in: Schörnig, Niklas/Reinhold, Thomas (eds): *Armament, Arms Control and Artificial Intelligence: The Impact of Software, Machine Learning and Artificial Intelligence on Armament and Arms Control*, 27–38.
- Rosert, Elvira/Sauer, Frank. 2021. "How (not) to stop the killer robots: A comparative analysis of humanitarian disarmament campaign strategies", in: *Contemporary Security Policy* 42 (1): 4–29.

- Sauer, Frank. 2021. "Stepping back from the brink: Why multilateral regulation of autonomy in weapons systems is difficult, yet imperative and feasible", in: *International Review of the Red Cross* 102 (913): 235–59.
- Boulanin, Vincent/Davison, Neil/Goussac, Netta/Peldán Carlsson, Moa. 2020. *Limits on Autonomy in Weapon Systems: Identifying Practical Elements of Human Control*, SIPRI and ICRC.
- Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War*.
- Götttsche, Malte/Daase, Christopher. 2024. *CNTR Monitor 2024. Perspectives on Dual Use*
- CNTR Monitor 2024. Perspectives on Dual Use [https://www.cntrarmscontrol.org/fileadmin/Medien/Monitor/CNTR_Monitor_2024_EN_web.pdf]

Internet resources

- www.icrac.net [<https://www.icrac.net/>]
- [www.prif.org](https://www.prif.org/en/research/cntr) [<https://www.prif.org/en/research/cntr>]
- [www.nato.int](https://www.nato.int/cps/bu/natohq/topics_18) [https://www.nato.int/cps/bu/natohq/topics_18]

4303.htm]

- [www.cto.mil](https://www.cto.mil/usdre-strat-vision-critical-tech-areas/) [<https://www.cto.mil/usdre-strat-vision-critical-tech-areas/>]

Who to follow on BlueSky or X:

- @cyberpeace1.bsky.social
- @drfranksauer.bsky.social
- @niklasschoernig.bsky.social
- @profbode.bsky.social
- @peasec.de
- @cntrarmscontrol.org
- @michaelhorowitz.bsky.social
- @drfranksauer
- @IngvildBode
- @BanKillerRobots
- @sambendett
- @DefTechPat
- @TobyWalsh
- @FLlrisk
- @niklasschoernig

1. [https://www.eeas.europa.eu/delegations/un-geneva/ccw-gge-laws-eu-ltts_en?s=62]