



UNIDIR



Funded by
the European Union

PRIMER

Electronic Warfare and Innovations in Uncrewed Aerial Systems: Arms Control and Disarmament Implications

MERSINI MARKOPOULOU • FEDERICO MANTELLASSI



Acknowledgements

Support from UNIDIR funders provides the foundation for all of the Institute's activities. This study was funded by the European Union as part of the Science and Technology Watchtower project and implemented by UNIDIR's Security and Technology Programme (SECTEC), which is supported by Germany, Italy, the Netherlands, Switzerland and Microsoft.

The authors would like to thank the experts who participated in interviews and shared their insights over the course of this research, as listed in Appendix A. The authors are also grateful to the experts who reviewed the report and provided valuable comments and suggestions including Dr. Yasmin Afina, Sarah Grand-Clément, Dr. Giacomo Persi Paoli, Ioana Puscas, Ioannis Vagias and Dr. Thomas Withington. Their input meaningfully strengthened this study.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. It is based in Geneva and assists the international community in developing the practical, innovative ideas needed to find solutions to critical security problems.

About the Security and Technology Programme

Contemporary developments in science and technology present new opportunities for, as well as challenges to, international security and disarmament. UNIDIR's Security and Technology Programme aims to build knowledge and awareness about the international security implications and risks of specific technological innovations and convenes stakeholders to explore ideas and develop new thinking on ways to address them.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Citation

Markopoulou, Mersini and Federico Mantellassi, *Electronic Warfare and Innovations in Uncrewed Aerial Systems: Arms Control and Disarmament Implications*. Geneva, UNIDIR, 2026.

Cover image: A drone hovers in a smoky, dark environment, illuminated by an explosive, glowing network of connected blue lights.

Created with AI by Anca.

About the authors



Mersini Markopoulou

Mersini Markopoulou was an Associate Research Consultant with UNIDIR's Security and Technology Programme. Her work focuses on the intersection of international security and emerging technologies, with an interest in electromagnetic and sensing technologies. She holds a master's degree in security and resilience from Imperial College London and a bachelor's degree in law from the University of Leeds.



Federico Mantellassi

Federico Mantellassi is a Researcher with UNIDIR's Security and Technology Programme. His work focuses on the international security implications, risks and opportunities of emerging science and technology developments and innovations. Previously, Federico was a Research and Project Officer at the Geneva Centre for Security Policy (GCSP), conducting research on the intersection of emerging technologies, international security and warfare. He holds a master's degree in intelligence and international security from King's College London and a bachelor's degree in international studies from the University of Leiden.

Acronyms and abbreviations

AI	Artificial intelligence
C2	Command and control
CRPA	Controlled reception pattern antennas
DEWs	Directed energy weapons
EMS	Electromagnetic spectrum
ESM	Electronic support measure
EW	Electronic warfare
GGE	Group of Governmental Experts
GNSS	Global navigation satellite system
ICT	Information and communications technology
IHL	International humanitarian law
INS	Inertial navigation system
LAWS	Lethal autonomous weapon systems
LEO	Low Earth orbit
OEWG	Open-Ended Working Group
PNT	Position, navigation and timing
RF	Radio frequency
SIGINT	Signals intelligence
UAS	Uncrewed aerial system

Table of contents

Executive summary	6
1. Introduction	8
1.1 Purpose and scope	10
1.2 Primer structure	10
2. The electromagnetic spectrum and electronic warfare	11
2.1 The electromagnetic spectrum	11
2.2 Electronic warfare	13
2.3 Emerging developments in electronic warfare	16
3. Use of electronic warfare against UASs and related innovation pathways	18
3.1 The use of electronic warfare against UASs	18
3.2 Electronic warfare as a driver of UAS innovation	20
4. Implications for international peace and security, arms control and disarmament	26
4.1 Lethal autonomous weapon systems	27
4.2 Proliferation risks	28
4.3 Monitoring and verification challenges	29
4.4 UAS governance	30
5. Conclusion	31
Appendix A. List of interviewees	33

Executive summary

The electromagnetic spectrum (EMS) has become a key enabler of modern military operations. With the increase in the number and types of capabilities that rely on the EMS for communications, navigation, sensing and guidance, the contest to control the EMS has become a central and growing aspect of military operations. While not new, “electronic warfare” (EW) is now a persistent, distributed and increasingly accessible feature of modern conflicts. It has accelerated a dynamic between measures and countermeasures, whereby developments to disrupt the EMS are matched by developments that seek to overcome these disruptions. This primer examines how two core EW techniques – jamming and spoofing – are driving innovations in the design and use of uncrewed aerial systems (UASs) and considers the implications of this dynamic for disarmament, arms control and international security.

UASs are particularly exposed to electronic warfare as both their command-and-control (C2) links and the signals from a global navigation satellite system (GNSS) that underpin their navigation, communication and targeting can be jammed or spoofed. The effects can range from loss of situational awareness to a UAS being steered off course by an attacker. The growing prevalence of UASs in modern conflicts, combined with their vulnerability, has made them one of the clearest arenas where a cycle of measure and countermeasure is unfolding between EW and weapon systems.

In response to their vulnerability, militaries and industry are developing a wide range of technologies to make UASs more resilient. These include:

- ▶ Anti-jamming and anti-spoofing techniques and low-probability-of-detection communications, or the use of fibre-optic cables to protect the C2 link
- ▶ Complementary, non-radio-frequency positioning methods (e.g., controlled reception pattern antennas, multi-constellation receivers and terrain-matching) to reduce dependence on GNSS
- ▶ Artificial intelligence (AI), which is increasingly used to process sensor data, to support autonomous navigation and target recognition, and to allow systems to continue operating with reduced or no reliance on external signals

These innovations are frequently layered together. While several remain at the testing or development stage, they are already reshaping the direction of UAS development. In particular, they point to the emergence of systems that are capable of operating with reduced, minimal or no dependence on continuous external inputs.

Electronic warfare is therefore a force that is shaping the development of UASs and military capabilities more broadly. This dynamic carries several implications for international peace and security, disarmament and arms control. First, it intersects directly with ongoing discussions on lethal autonomous weapon systems (LAWS) as EW-affected environments create strong pressures on militaries to field more autonomous systems while complicating questions of human control. Second, the dual-use nature of many of the technologies involved raises proliferation risks, for the diffusion of both powerful EW capabilities and EW-resistant countermeasures to non-State actors, while in turn driving further development of physical counter-UAS measures such as directed energy weapons. Third, the software-defined nature of many EW-related technologies and the pace of innovation make monitoring and

verifying capabilities increasingly difficult since systems can be reconfigured or enhanced without visible changes to hardware. Finally, these dynamics bear on existing governance efforts for UASs, which focus chiefly on tracking the transfer of systems and their components, rather than on the qualitative developments that may affect their risk profile.

As EW continues to shape the design, deployment and operational use of UASs, the disarmament and arms control community would benefit from closer and more systematic engagement with this dynamic. Considerations for further attention include:

- ▶ Following developments in EW to further understand how they will shape the operational environment of LAWS and how this will affect the modalities of human control
- ▶ Monitoring the proliferation of dual-use EW and EW-resistant technologies, including to non-State actors, and their knock-on effects on counter-UAS development
- ▶ Exploring approaches to monitoring and verification that can account for the software-defined and rapidly evolving nature of EW-related capabilities
- ▶ Considering how EW-driven qualitative developments in UASs should inform existing governance frameworks on the transfer, export and use of uncrewed systems



Battlefield and network. Hybrid war. By Metamorworks

1. Introduction

Modern militaries depend on the electromagnetic spectrum (EMS), which is made up of different types of electromagnetic radiation. Electromagnetic radiation takes the form of electromagnetic waves which, in turn, enable core military functions such as command and control (C2), intelligence, surveillance and reconnaissance (ISR), navigation and positioning, weapon guidance, and battlefield networking.

The central role played by the EMS in the military domain has been described as “the invisible . . . and physical foundation of every battlefield – it unifies all the warfighting domains: land, air, sea, space, and cyberspace. In fact, it is the only physical space shared by every warfighter”.¹ Because the EMS plays such a central role in the military domain and for military action, it is also an area of competition. Militaries do not merely depend on the EMS; they actively compete within it, seeking to secure their own use of it while limiting that of their adversaries.² This dynamic has long been a feature of warfare, but the significance of the EMS has grown alongside the increasing reliance of military systems on electromagnetic functions and wireless networking. Operations conducted in and through the EMS are

1 W.R. Alan Dayton, “Winning the invisible fight: The need for spectrum superiority”, Defense 360, Center for Strategic and International Studies (CSIS), 21 December 2016, <https://defense360.csis.org/wp-content/uploads/2016/12/Transition45-Dayton-Spectrum-Superiority-1.pdf>, 1.

2 US Department of Defense, “Electromagnetic spectrum superiority strategy”, October 2020, https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/electromagnetic_spectrum_superiority_strategy.pdf.

commonly referred to as electronic or electromagnetic warfare (EW). This refers to techniques “which seek to deny, impede or destroy an adversary’s ability to access the electromagnetic spectrum”.³

The issue of EW as an international security challenge is not new. At the multilateral level, discussions touching upon EW have primarily centred on its non-kinetic effects, attribution challenges and impact on infrastructure. For example, EW has been discussed from the perspectives of outer space security and of information and communications technologies (ICTs) in the context of international security. Early attention to EW-related capabilities emerged in the Group of Governmental Experts (GGE) on further practical measures for the prevention of an arms race in outer space (2018–2019), where EW was recognized as a threat to space systems.⁴ This focus was expanded in the Open-Ended Working Group (OEWG) on reducing space threats through norms, rules and principles of responsible behaviours (2022–2023), which acknowledged the potential of EW (jamming and spoofing) as non-kinetic anti-satellite (ASAT) weapons.⁵ With regards to ICTs, both final reports of the OEWG on developments in the field of ICTs in the context of international security (2025) and of the GGE on advancing responsible State behaviour in cyberspace in the context of international security (2021) use broad language, such as “harmful ICT activities” and “the growing use of ICTs for malicious purposes”.⁶ While neither of these processes explicitly refers to jamming or spoofing, research has recognized that ICTs can enable EW.⁷

However, these examinations of EW by the international community have not focused on how EW drives military capabilities more broadly. Yet, EW has been identified as “driving innovation in electronic warfare-resistant systems across . . . navigation, communications and sensing”.⁸ Nearly every weapon system now depends on the EMS to operate, while EW has the potential to interfere with anything on the battlefield that depends on the EMS – from radio communications and radars, to global navigation satellite systems (GNSSs) and the systems that rely on them.⁹ This dependency on the EMS thus creates a vulnerability: without continuous and reliable access to it, these systems cannot function as intended. In response, militaries are pursuing innovations aimed at increasing the resilience of weapon systems through EW-resistant technologies and, in some cases, reducing dependence on the EMS through greater autonomy. Exploring this interaction between EW and

3 General Assembly, “Current developments in science and technology and their potential impact on international security and disarmament efforts”, Report of the Secretary-General, A/80/237, 22 July 2025, <https://docs.un.org/A/80/237>, paragraph 59.

4 General Assembly, Report of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space, A/74/77, 9 April 2019, <https://docs.un.org/A/74/77>.

5 General Assembly, Open-Ended Working Group on reducing space threats through norms, rules, and principles of responsible behaviours, Chairperson’s summary, A/AC.294/2023/WP.22, 1 September 2023, <https://docs.un.org/A/AC.294/2023/WP.22>; “Non-kinetic anti-satellite weapons”, Submitted by the Outer Space Institute Working Group on Space Security, A/AC.294/2023/NGO/1, 13 January 2023, <https://docs.un.org/A/AC.294/2023/NGO/1>.

6 General Assembly, final report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, A/AC.292/2025/L.1; General Assembly, Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security, A/76/135, 14 July 2021, <https://docs.un.org/A/76/135>.

7 Kerstin Vignard (ed.), “ICTs and International Security”, *Disarmament Forum*, no. 3 (September 2007), <https://unidir.org/wp-content/uploads/2023/09/icts-and-international-security-en-332.pdf>.

8 General Assembly, A/80/237, paragraph 61.

9 Interview with Thomas Withington.

weapon systems is therefore essential for understanding contemporary military innovation and its implications for international security as well as for disarmament and arms control.

1.1 Purpose and scope

This primer examines how EW affects modern weapon systems and how it is driving military innovation. Due to their growing relevance in modern conflicts and in the context of EW, the primer specifically considers innovations related to **uncrewed aerial systems (UAS)**. In the context of this primer, UAS refers to a remotely piloted and semi-autonomous platform, including its navigation and communications subsystems. The primer also explores the implications that these developments could pose for disarmament, arms control and international security more broadly.

While EW encompasses a range of techniques, this primer focuses specifically on **jamming and spoofing**. These were selected because both techniques are based on radio frequency (RF) and act on the functioning of systems by degrading, denying or manipulating the data or connectivity on which a system relies. These non-kinetic first-order effects may produce downstream physical effects (e.g., where a spoofed or jammed system loses control and crashes).¹⁰

The primer was developed using open-source information. It does not contain, nor was it based on, information classified by national governments or military authorities. The study involved three activities:

- ▶ First, relevant literature related to the evolution of EW, its employment against weapon systems and the responding innovations in these systems was reviewed.
- ▶ Second, interviews were conducted between February and April 2026 with 15 individuals with experience in EW, military innovation, disarmament and arms control working in non-profit organizations, academia and research organizations (see full list in Appendix A).
- ▶ Third, developments related to EW between 1 January 2025 and 1 April 2026 were monitored.

1.2 Primer structure

This primer is divided into a further four sections. Section 2 provides an overview of the EMS and the evolution of EW in conflict environments. Section 3 explores how EW is employed against UASs, and the impacts this has on their performance, before illustrating how EW has influenced innovation in UASs and the role of emerging technologies in enabling this innovation. Finally, Section 4 considers potential intersections of these innovations with disarmament, arms control and international security more broadly. The primer concludes in Section 5.

10 Joint Air Power Competence Centre (JAPCC), *A Comprehensive Approach to Countering Unmanned Aircraft Systems* (Kalkar: JAPCC, January 2021), <https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf>.

2. The electromagnetic spectrum and electronic warfare

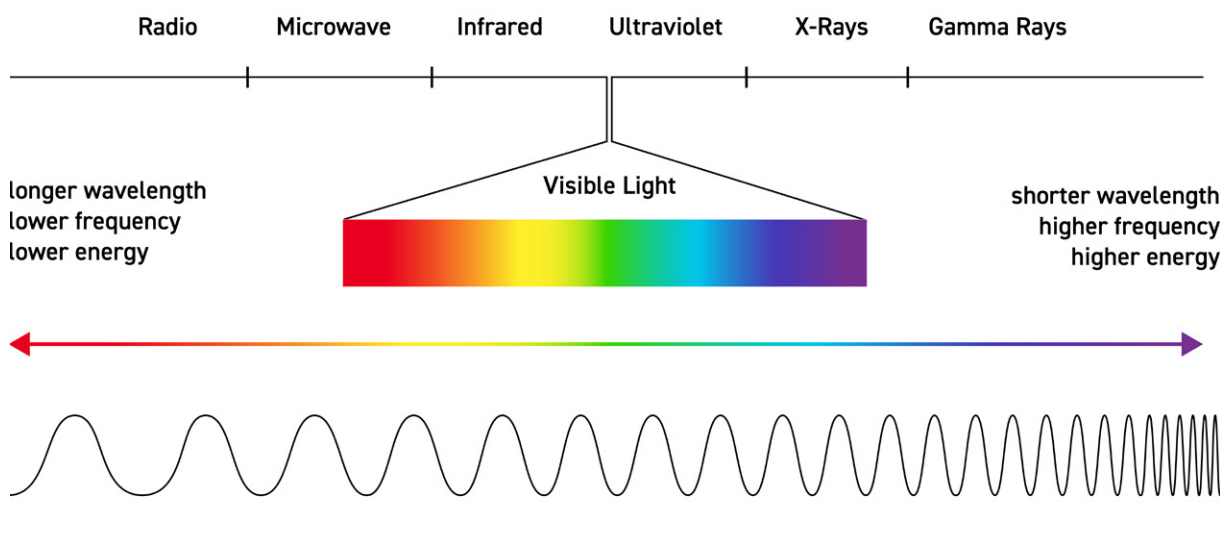
This section describes the electromagnetic spectrum and the functions that it enables. It explains how electronic warfare functions, the associated hardware and software it relies on, and why EW may be employed instead of kinetic action in certain circumstances. The section also examines how emerging technologies, particularly artificial intelligence (AI) and quantum technologies, are converging with EW.

2.1 The electromagnetic spectrum

The EMS refers to the range of all electromagnetic radiation. These include radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays and gamma rays, each distinguished by a specific frequency and wavelength (see Figure 1).¹¹ For military applications, the most useful regions of the spectrum are radio waves, microwaves and infrared radiation.¹² These regions of the spectrum combine the abilities to carry information, travel long distances and interact with the physical environment in a way that makes them suitable for military functions. For example, radio waves enable both

FIGURE 1

The electromagnetic spectrum¹³



11 US National Aeronautics and Space Administration (NASA), Goddard Space Flight Center, "The electromagnetic spectrum", March 2013, <https://imagine.gsfc.nasa.gov/science/toolbox/emspectrum1.html>.

12 Michael Mayer, *Electromagnetic Warfare on the Current and Future Battlefield*, Norwegian Defence Research Establishment (FFI) Report 26/016 (Kjeller: FFI, 27 March 2026), <https://www.ffi.no/en/publications-archive/electromagnetic-warfare-on-the-current-and-future-battlefield>.

13 N. Hanacek/NIST, "Electromagnetic spectrum graphic", US National Institute of Standards and Technology (NIST), 11 September 2024, <https://www.nist.gov/image/electromagnetic-spectrum-graphic>.

long-range and short-range communications, microwaves support radar by reflecting off objects,¹⁴ and infrared radiation allows the detection of heat signatures.

The same regions of the EMS also underpin the functions on which weapon systems depend, such as:

- ▶ **Communications:** This enables the exchange of information (e.g., sensor data and voice traffic) between platforms, weapon systems, sensors, bases, computer systems and personnel, thereby supporting coordination, command and control, and situational awareness.
- ▶ **Position, navigation and timing (PNT):** This enables a system to determine its location, orientation and precise timing, thereby supporting navigation, synchronization and targeting. The EMS is a conduit for PNT relying on GNSS signals; other forms of PNT provision are available to militaries that do not need the EMS (e.g., atomic clocks and inertial navigation systems).
- ▶ **Sensing:** This enables the detection, identification, tracking and characterization of targets using sensors such as radar, lidar or cameras.
- ▶ **Guidance:** This enables a system to steer towards a target by processing radio navigation and sensor data and generating control commands for trajectory correction and target interception.

The operation of these functions depends on their ability to generate, transmit, receive and detect electromagnetic signals (see Box 1).

BOX 1

Key terms explained: Signal, system and link

A **signal** is information imposed on an electromagnetic wave. An electromagnetic wave by itself carries no message, it simply exists. To make it useful, a transmitter, with the help of an antenna, modifies one of the properties of the wave (i.e., its amplitude, frequency or phase). This process is known as modulation. At the other end, a receiver reverses the process; it reads the modulation pattern and reconstructs the original information.¹⁵ With modulation, an electromagnetic wave becomes a signal. Signals can convey different types of information: commands issued by an operator to direct a system's behaviour; data gathered by on-board sensors and relayed back to the operator; or positioning and timing information. In effect, signals form the link between operator decision-making and physical action on the battlefield.

A **system** is something that acts on a signal to perform a particular action. It receives input signals, processes them, and produces output signals or responses. In military contexts, many EMS-dependent weapon systems rely on transmitting and receiving signals to function as intended.

A **link** is a communication channel that allows signals to be transmitted between two or more transmitters and receivers.

14 Note that some radars also exploit radio signals below the microwave band (i.e., below 300 megahertz).

15 Otto H. Muller, "Modulation", EBSCO, 2022, <https://www.ebsco.com/research-starters/engineering/modulation>.

2.2 Electronic warfare

Electronic warfare encompasses techniques “which deny, impede or destroy an adversary’s ability to access the electromagnetic spectrum”.¹⁶ EW is not a new concept; it has developed alongside the technologies on which militaries have come to depend, growing in sophistication as those dependencies deepened. Early EW focused primarily on intercepting and analysing enemy radio communications to understand force structure, movements and intentions.¹⁷ It remained passive, focusing on information collection, rather than actively interfering with enemy systems. The widespread adoption of technologies such as radar, navigation and guidance thus created new opportunities, but also exposed the vulnerabilities of EMS-dependent functions. EW came of age during the Second World War as militaries began employing jamming and spoofing techniques to interfere with these functions while also developing countermeasures to protect their own systems.¹⁸ EW therefore evolved into a dynamic cycle of measures and countermeasures.

The dependence of military systems on functions enabled by the EMS has expanded significantly. Modern weapon systems depend on continuous data exchange, sensor integration and precision navigation, which makes access to the EMS essential for their effectiveness. It is within this context that EW has evolved. In modern warfare, EW has become a persistent and distributed feature of military operations, rather than an episodic support tool. “Persistent” in this context means that EW is no longer employed only at specific moments but is a permanent feature of the operational environment.¹⁹ The term “distributed” reflects the proliferation of smaller, mobile platforms capable of carrying EW equipment, which allows interference to be applied across multiple points simultaneously.²⁰ EW capabilities have also become more accessible: the commercial availability of EW equipment has lowered the barriers to acquiring equipment that would have been difficult to produce only a decade ago.²¹ Taken together, these developments reinforce a central dynamic: as military reliance on the EMS increases, so too does the attack surface available to EW. Electronic warfare itself continues to evolve within this context, and its impact grows accordingly.

To date, there is no single agreed-upon categorization of EW. However, it is typically divided into three broad categories: support (sometimes termed surveillance), attack and defence.²²

16 General Assembly, A/80/237, paragraph 59.

17 Lieutenant George Hageman, “Battle of Tsushima: The first naval battle of the 21st century”, US Naval History and Heritage Command, 2020 <https://www.history.navy.mil/get-involved/essay-contest/2020-winners/hageman-cno-essay.html>; Wilhelm Flicke, “The beginnings of radio intercept in World War I: A brief history by a German intelligence officer”, *Cryptologic Spectrum*, vol. 8, no. 2 (summer 1978), https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-spectrum/beginnings_radio_intercept.pdf.

18 Robert Hutton, “Battle of the Beams: Germany’s invisible secret weapons that could have devastated Britain”, History Net, 10 July 2021, <https://historynet.com/battle-of-the-beams-the-time-germany-devised-an-invisible-weapon-that-could-devastate-britain/>; Gareth Evans, “The evolution of electronic warfare: A timeline”, Army Technology, 7 June 2018, <https://www.army-technology.com/features/evolution-electronic-warfare-timeline/?cf-view>.

19 Interview with the Royal Institute of Navigation; Interview with Warren Du Plessis.

20 Interview with Mireille Elhajj; Interview with Ioannis Vagias.

21 Interview with the Royal Institute of Navigation.

22 The terms surveillance, attack and defence are used here in their standard military-technical sense within electronic warfare. They do not imply a legal characterization of a specific act under international law.

- ▶ **Support:** Any system that uses electromagnetic signals must emit, reflect or receive those signals. Hence, dependence on the EMS carries an inherent vulnerability as the signals can be detected and analysed through signals intelligence (SIGINT). Analysis of these signals can reveal the presence of a weapon system, its general function (e.g., whether a signal originates from a radar or a communications system) and its approximate location.²³
- ▶ **Attack:** This category involves the use of electromagnetic emissions to disrupt or degrade enemy systems (see Box 2). The most common techniques are jamming and spoofing.
 - ▶ **Jamming** degrades or denies a receiver's ability to extract information by overwhelming it with an interfering signal.²⁴ A jammer transmits an interfering signal on the same frequency as the targeted signal, raising the noise level at the receiver end until the original signal can no longer be interpreted.
 - ▶ **Spoofing** generates a signal that mimics the signal that the receiver expects, but carries manipulated content about the object's position, speed or timing.²⁵ It is generally more complex than jamming.
- ▶ **Defence:** Measures can be taken to protect systems against the effects of an attack. This includes techniques to resist or mitigate jamming, as well as techniques to detect and reject spoofed signals.²⁶

The use of EW by military actors is growing as it is perceived as providing operational advantages in terms of speed, cost, attribution and controllability of effects. First, as an EMS-based technique, EW attacks propagate at the speed of light. This enables the instantaneous disruption of systems within the effective range of the attack. Second, EW attacks can often be employed at relatively low cost. For example, commercially available jammers marketed as privacy devices have the power to jam GNSS signals within hundreds of metres.²⁷ Third, EW attacks can be difficult to attribute with certainty as they rely on invisible electromagnetic emissions. As such, identifying the source of interference can be technically challenging, particularly in complex operational environments where other electromagnetic emissions are present.²⁸ Fourth, the first-order effects of EW attacks are often temporary and reversible. Unlike kinetic attacks, they do not cause permanent physical damage to the targeted system, which allows operators to adjust both the level and duration of the disruptive effects.²⁹ Nonetheless, it is important to recognize that the second- and third-order downstream effects of an EW attack may be physical, including harm to civilian infrastructure or to civilians.

23 Jack Watling and Noah Sylvia, *Competitive Electronic Warfare in Modern Land Operations* (London: Royal United Services Institute, January 2025), https://static.rusi.org/competitive-electronic-warfare-in-land-operations_1.pdf; Stephanie Halwa and Lydia Harris, "Electromagnetic (electronic) warfare", POSTnote no. 749, Parliamentary Office of Science and Technology (POST), British Parliament, 10 July 2025, <https://doi.org/10.58248/PN749>.

24 Joint Air Power Competence Centre, *A Comprehensive Approach to Countering Unmanned Aircraft Systems*.

25 Joint Air Power Competence Centre, *A Comprehensive Approach to Countering Unmanned Aircraft Systems*.

26 Watling and Sylvia, *Competitive Electronic Warfare in Modern Land Operations*.

27 Sony Semiconductor Solutions, "What is GNSS jamming and spoofing? How to detect and defend", 19 June 2025, <https://www.sony-semicon.com/en/products/lsi-ic/gps/blog/20250619.html>.

28 Clayton Swope et al., *Space Threat Assessment 2025* (Washington, DC: Center for Strategic and International Studies), 2 April 2025, <https://www.csis.org/analysis/space-threat-assessment-2025>.

29 Tyler Way, "Counterspace weapons 101", Center for Strategic and International Studies, 14 June 2022, <https://aerospace.csis.org/aerospace101/counterspace-weapons-101/>.

The anatomy of an electronic warfare attack

An electronic warfare attack is composed of a series of steps, involving both hardware and software components.

- ▶ **Detection:** An electronic support measure (ESM) uses a receiver to constantly scan the surrounding environment for signals (e.g., radar or communications emissions).
- ▶ **Sampling:** The receiver captures these signals and passes them into the processing hardware for examination.
- ▶ **Analysis:** The processing hardware examines the signal's properties to work out its identity, type and origin and whether it constitutes a threat.³⁰ In older systems, many of which remain in active use, identification is performed by comparing the signal against preloaded threat libraries of known enemy, friendly and neutral signals. If the signal is not in the library, it goes unrecognized and may be sent to SIGINT experts for further analysis.³¹ Modern systems may use AI to analyse unfamiliar signals in real time.³²
- ▶ **Respond:** If the signal is identified as a threat, an electronic attack system (which may or may not be collocated with the ESM) may generate a response using software-defined radios to produce either jamming or spoofing signals.³³
- ▶ **Transmit:** Finally, the transmitter directs the response signal towards the target.

30 Everything RF, "Electronic warfare", 2025, https://cdn.everythingrf.com/live/Electronic_Warfare_eBook_2024_638646752293473148_1_3_638760766145874076.pdf.

31 Feridun Taşdan, *Electronic Warfare: Global Trends & Turkish Capabilities Report* (Ankara: SETA, 2022), <https://media.setav.org/en/file/2022/07/electronic-warfare-global-trends-turkish-capabilities-report-seta-emerging-military-technologies....pdf>.

32 Matt Thompson, "Unlocking the strategic potential: Artificial intelligence in electronic warfare", *Journal of Electromagnetic Dominance*, 2023, <https://www.jedonline.com/2023/09/13/unlocking-the-strategic-potential-artificial-intelligence-in-electronic-warfare/>.

33 Everything RF, "Electronic warfare". A software-defined radio is a radio communication system that uses software to process signals, rather than relying on fixed physical components. This makes software-defined radios highly flexible, as they can be reconfigured to operate across a wide range of frequencies and signal types.

2.3 Emerging developments in electronic warfare

Electronic warfare is progressing from a technological point of view and will increasingly operate in conjunction with other emerging technologies, in particular AI and quantum technologies.

The integration of AI into EW, often framed as “cognitive EW”, has emerged in response to the growing complexity of the electromagnetic environment. Modern operational settings involve vast volumes of signals across multiple frequencies, making real-time analysis and response increasingly difficult. AI enables EW systems to process large volumes of signals rapidly, identifying patterns and anomalies that would otherwise be difficult to detect.³⁴ Machine learning techniques can support the accurate classification of signals.³⁵ Deep neural networks, for instance, is a machine learning technique capable of identifying patterns in large volumes of data. When integrated into EW, deep neural networks enable EW systems to detect subtle variations in signal characteristics, which enhances both detection and identification capabilities.³⁶ Importantly, AI also enables greater autonomy in EW systems: it allows systems to respond to unprogrammed threats and to adapt their behaviour in real time.³⁷ Furthermore, techniques such as reinforcement learning allow EW systems to optimize jamming or deception strategies dynamically, based on continuous feedback from the environment.³⁸ Overall, AI integration is expected to accelerate decision-making cycles and enhance the responsiveness of EW. (On the implications of the increased convergence between AI and EW see Box 3.)

The integration of quantum technologies into EW remains at an early stage of development, with most applications being in the experimental phase. Nevertheless, these technologies have the potential to reshape key aspects of EW in the longer term. For example, quantum sensing could enable highly precise measurements of electromagnetic signals, which would allow for the detection of extremely weak emissions and improve performance in complex electromagnetic environments.³⁹ This could translate into greater detection ranges and increased sensitivity against low-observable or low-probability-of-intercept systems. Thus, quantum computing holds potential relevance for EW, particularly in relation to the rapid processing and analysis of complex signals, as well as the possible acceleration of the process of decrypting adversary communications.⁴⁰ Overall, these capabilities indicate a trajectory in which both sensing and signal exploitation in EW could become more powerful.

34 Thomas Courtat et al., AI for Electromagnetic Warfare (Meudon: Thales Group, n.d.) [https://www.thalesgroup.com/sites/default/files/2026-04/AI for Electronic Warfare_0.pdf](https://www.thalesgroup.com/sites/default/files/2026-04/AI%20for%20Electronic%20Warfare_0.pdf).

35 Louis Lesieur et al., “An overview and classification of machine learning approaches for radar signal deinterleaving”, IEEE Access, vol. 13 (January 2025), <https://doi.org/10.1109/ACCESS.2025.3539589>.

36 Nicolae Sfetcu, “Challenges and risks of artificial intelligence in electronic warfare”, IT & C, vol. 4, no. 1 (March 2025), <https://doi.org/10.58679/it26925>.

37 Thompson, “Unlocking the strategic potential”.

38 Sfetcu, “Challenges and risks of artificial intelligence in electronic warfare”.

39 Michal Krelina, “An introduction to military quantum technology for technology policymakers”, SIPRI, March 2025, <https://doi.org/10.55163/DRDQ1599>; David L. Chandler, “Quantum sensor can detect electromagnetic signals of any frequency”, MIT Department of Physics, 20 June 2022, <https://physics.mit.edu/news/quantum-sensor-can-detect-electromagnetic-signals-of-any-frequency/>.

40 Salvador Álvarez, “Electronic warfare: The silent battlefield of the future”, Grupo Oesia, n.d., <https://grupooesia.com/en/insight/electronic-warfare-the-silent-battlefield-of-the-future/>.

Implications of the convergence between artificial intelligence and electronic warfare

While the integration of artificial intelligence in electronic warfare may provide substantial operational benefit, AI-enabled EW systems will suffer from challenges and risks similar to those linked to the broader integration of AI systems in the military domain.⁴¹ These include issues related to data scarcity, quality and bias, adversarial manipulation, explainability and transparency, robustness, and reliability among others.⁴² In addition, the progressive integration of AI into EW functions raises concerns about reduced human oversight over EW.

The importance of EMS dominance in modern warfare will continue to grow, and critical advantages will be gained by the integration of AI in EW.⁴³ In this context, discussions surrounding AI in the military domain should give specific attention to – and foster a deeper understanding of – how AI affects the contest over the EMS. Indeed, EW does not feature prominently in debates surrounding AI in the military domain. As AI makes further inroads in the conduct of EW, a deeper understanding of the impacts and risks is necessary. This is true for understanding the implications of increasingly autonomous EW, for the necessary policy and technical guardrails, and for the standards and norms that are necessary for the safe, secure and responsible development of AI-enabled EW capabilities.

41 Sfetcu, “Challenges and risks of artificial intelligence in electronic warfare”.

42 *Ibid*

43 Dominika Kunertova, “How NATO can integrate AI to prevail in future algorithmic warfare”, Atlantic Council, 30 March 2026, <https://www.atlanticcouncil.org/in-depth-research-reports/report/how-nato-can-integrate-ai-to-prevail-in-future-algorithmic-warfare/>.

3. Use of electronic warfare against UASs and related innovation pathways

3.1 The use of electronic warfare against UASs

UASs have become a defining feature of modern conflicts.⁴⁴ While the extent of their impact on warfare remains debated, their number, use, sophistication and variety have certainly increased in recent years.⁴⁵ Despite their growing importance, their use in conflict settings has been strongly affected by, among other things, their vulnerability to EW.⁴⁶ At the same time, the importance of EW capabilities has been reinforced by the threat posed by UASs.⁴⁷ Therefore, UASs represent one of the areas where the cycle of innovation between weapon systems and EW has been particularly prominent, visible and relevant.

This section analyses how EW is used against UASs. It first focuses on how EW affects UASs' dependency on signals or links that enable functions such as remote control and transfer of sensor data, and then examines how EW affects the functioning of UASs. It should be noted that these impacts are explained in a general sense; whether and how a UAS is affected ultimately depends on its specific design features, with some systems being more resistant to jamming and spoofing than others. Moreover, UASs can be employed for either civilian or military purposes. In principle, all types of UAS are potentially vulnerable to EW, unless explicitly designed to operate in environments where the electromagnetic spectrum is highly contested. However, UASs intended for civilian use are generally more susceptible as they usually lack built-in resistance to such interference.⁴⁸

The operation of a UAS depends on a **command-and-control link** and **GNSS signals**. The C2 link enables two-way wireless communication between the operator and the UAS. It is divided into an uplink and a downlink (where “up” and “down” refer to the direction of data flow, not the physical direction).

44 Volodymyr Pavlov and Dan Peleschuk, “Drones dominate Ukraine battlefield four years into fighting”, Reuters, 24 February 2026, <https://www.reuters.com/business/aerospace-defense/drones-dominate-ukraine-battlefield-four-years-into-fighting-2026-02-24/>.

45 Stacie Pettyjohn, *Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine* (Washington, DC: Centre for a New American Security, February 2024), <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Defense-Ukraine-Drones-Final.pdf>; Sarah Grand-Clément, “Armed and dangerous? A brief overview of uncrewed aerial systems: Risks, impacts, and avenues for action”, UNIDIR, 2024. https://unidir.org/wp-content/uploads/2024/10/armed_and_dangerous_web.pdf.

46 Jack Watling and Nick Reynolds, *Tactical Developments during the Third Year of the Russo-Ukrainian War* (London: Royal United Services Institute, February 2025), <https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf>.

47 Watling and Sylvia, *Competitive Electronic Warfare in Modern Land Operations*; Jake Epstein, “A Ukrainian defence firm says electronic warfare demand is surging as Russia launches strike drones every minute”, Business Insider, 31 July 2026, <https://www.businessinsider.com/ukrainian-company-says-electronic-warfare-demand-surging-fight-russia-drones-2026-7>.

48 Aaron Yu et al., “Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics: A survey”, Arxiv, 10 April 2025, <https://arxiv.org/html/2504.07358v1>.

The uplink is the signal transmitted from the operator to the UAS. It carries flight commands, mission updates and operational instructions. The downlink is the signal travelling from the UAS back to the operator. It carries data collected by the UAS, such as videos, pictures and telemetry (height, speed).⁴⁹ GNSS signals are one-way signals that the UAS passively receives from satellites (GNSS refers to any satellite constellation that provides global positioning, navigation and timing services, e.g., BeiDou, Galileo, GLONASS, GPS).⁵⁰ These signals provide position and timing information necessary for the UAS to know its location. EW can therefore target either the C2 link or the GNSS signals or both.

There are five different EW scenarios:

- ▶ If the **C2 uplink is jammed**, the operator can no longer send new commands. In such cases, a UAS does not necessarily crash or lose all functionality. Instead, from the moment that jamming occurs, it can enter a lost-link mode. This activates a preprogrammed response, which may include:
 - ▶ Returning to its take-off point (if GNSS is available)
 - ▶ Loitering or hovering in the air, waiting for the signal to be restored
 - ▶ Landing
 - ▶ Continuing its last programmed mission autonomously (usually a UAS intended for military use)⁵¹
- ▶ If the **C2 downlink is jammed**, the operator loses situational awareness entirely. This has no direct effect on the UAS's behaviour; it continues flying normally.
- ▶ If the **C2 uplink or downlink is spoofed**, false commands can be introduced. If successful, the UAS may respond to these commands instead of those from the legitimate operator. UASs that rely on insecure C2 links are thus more vulnerable to spoofing, while systems using encrypted links are more resistant.⁵²
- ▶ If **GNSS signals are jammed**, the UAS no longer knows where it is. If alternative on-board navigation systems are available, it might rely on them, often operating with reduced capability.
- ▶ If **GNSS signals are spoofed**, the UAS believes it is somewhere it is not. The UAS can then be steered by the attacker.⁵³

While this primer focuses on UASs, it is important to note that other weapon systems and components can be affected by EW (see Box 4).

49 UAV Navigation, "UAV navigation in depth: External datalink selection", Grupo Oesia, June 2018, <https://www.uavnavigation.com/company/blog/uav-navigation-depth-external-datalink-selection>.

50 UASs that are intended for civilian uses make use of civilian GNSS signals; these signals are unencrypted and unauthenticated, which makes them particularly vulnerable to EW attacks.

51 Younes Zidane, José Silvestre Silva and Gonalo Tavar , "Jamming and spoofing techniques for drone neutralization: An experimental study", *Drones*, vol. 8 no. 12 (December 2024), <https://doi.org/10.3390/drones8120743>; UAV Navigation, "UAV navigation in depth"; Interview with Ioannis Vagias; Interview with Mireille Elhajj.

52 Shah Zahid Khan, Mujahid Mohsin and Waseem Iqbal, "On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions", *PeerJ Computer Science*, vol. 7 (6 May 2021), <https://doi.org/10.7717/peerj-cs.507>; Jae Gu Kang and Byeong Cheol Choi, "Multi-modem-based FHSS-drone takeover with precision spoofing", *ETRI Journal*, vol. 47, no. 3 (June 2025), <https://doi.org/10.4218/etrij.2024-0369>.

53 Zidane et al., "Jamming and spoofing techniques for drone neutralization".

Electronic warfare impact beyond UASs

The operation of guided missiles depends on radar track information (i.e., where a target is and what it is doing). This is exchanged using a radio link between several components, including a target-tracking radar (providing target parameters), a fire control computer (generating commands based on the target and the missile's position) and the missile itself. This exchange enables the missile to determine the target's position and to guide itself towards that position. EW can therefore target the radar signals and the radio signals carrying track information on which the missile-guidance process relies.

Vulnerability to EW varies depending on the phase of flight of the missile (boost, mid-course, and terminal) and the types of guidance relevant for each phase (command and semi-active guidance). The mid-course phase, which is when the missile is guided towards the target, is generally most relevant from an EW perspective, as the missile depends on command guidance that can be interfered with during this phase. The terminal phase is also highly relevant to EW. For example, anti-ship missiles typically activate their own radars to confirm a target and its location as they approach. A surface-to-air or air-to-air missile may also activate a radar to guide towards the target during the terminal phase. In both cases, jamming and spoofing the missile becomes critically important.⁵⁴

Similarly, components such as precision guidance kits, which are add-on munition guidance upgrades for otherwise unguided systems (i.e., bombs, artillery shells), rely on employing GNSS and an inertial navigation system (INS).⁵⁵ If GNSS signals are jammed, the precision guidance kit can no longer receive external positioning information and must instead rely solely on its INS. Because INSs estimate position by integrating acceleration and rotation measurements over time, small sensor errors accumulate, causing that estimate to drift the longer the system operates without a GNSS fix. As a result, positioning accuracy gradually decreases during flight, and the uncertainty in the point of impact increases.⁵⁶

3.2 Electronic warfare as a driver of UAS innovation

The growing prevalence of EW has become an important driver of innovation in UASs, particularly in efforts to ensure these systems' ability to operate during attempted jamming or spoofing. Unlike threats that physically destroy or damage a platform, EW disrupts the communications, navigation and sensing

54 Training Support Squadron, "Electronic warfare fundamentals", US Air Combat Command, November 2020, <https://falcon.blu3wolf.com/Docs/Electronic-Warfare-Fundamentals.pdf>; David Hambling, "How spoofing is diverting Russian missiles into empty fields", *Forbes*, 20 November 2025, <https://www.forbes.com/sites/davidhambling/2025/11/20/how-spoofing-is-diverting-russian-missiles-into-empty-fields/>.

55 Thomas Withington, "Jamming JDAM: The threat to US munitions from Russian electronic warfare", Royal United Services Institute, 6 June 2023, <https://www.rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare>; Interview with Ioannis Vagias.

56 Withington, "Jamming JDAM"; Interview with Ioannis Vagias.

functions on which UASs rely. As a result, EW generates a measure–countermeasure dynamic in which efforts to disrupt weapon functions are continuously met by innovations designed to preserve operational effectiveness. The vulnerabilities of UASs identified above (in Section 3.1) – that is, C2 link vulnerability and GNSS signal vulnerability – are therefore the main points of adaptation around which innovations have emerged.

In addition, AI and autonomous mission execution are increasingly being explored as technological responses to EW, playing a cross-cutting and enabling role in addressing the identified vulnerabilities. While these technologies are addressed separately below (see Subsection 3.2.3), in practice they are often layered, meaning that they are applied in parallel to provide redundancy. This is particularly important for UASs, which may be simultaneously vulnerable to both C2 link and GNSS interference.

The innovations presented in this section include both advances that are already fielded as well as some that are still in testing or in developmental phases. Taken as a whole, these innovations illustrate how EW is shaping the evolution of the functions on which UASs and their components rely.

3.2.1 Command-and-control link vulnerability

The protection of the C2 link of a UAS is key.

One major area of UAS innovation is the **development of anti-jamming and anti-spoofing techniques** that seek to ensure that a UAS can continue exchanging data and commands even in the presence of EW. These techniques can also support communication between individual UASs.

A second area of innovation focuses on **reducing the detectability of the C2 link**. Rather than resisting interference, some systems attempt to minimize the likelihood that communications are detected in the first place. This can be achieved through techniques that lower the probability of detection or by shifting communications away from conventional radio frequency transmissions to other regions of the EMS or alternative physical media (e.g., cables). Developments in this area include spread-spectrum communications, ultra-wideband communications, beamformed communications, fibre-optic communications, laser communications, low Earth orbit (LEO) communications and mesh networking (see Table 1).

TABLE 1

Innovations in command-and-control links

Development	Description	Development status
Beamformed communications	Instead of broadcasting in all directions, a smart antenna focuses the signal into a narrow beam aimed at the intended transmitter or receiver end. This increases signal gain in the desired direction while reducing the probability of detection or jamming. The antennas must continuously track the receiver; there is a possibility that the antenna will lose its focus. ⁵⁷	Fielded

57 Krishnakanth Mohanta and Saba Al-Rubaye, “Integrated sensing and communication for UAV beamforming: Antenna design for tracking applications”, *Vehicles*, vol. 7, no. 4 (December 2025), <https://doi.org/10.3390/vehicles7040166>.

Development	Description	Development status
Fibre-optic communications	Data is transmitted as pulses of light through fibre-optic cable, rather than as radio waves. The C2 link cannot be jammed or intercepted easily. However, the physical cable limits range and mobility. ⁵⁸	Fielded
Laser communications	A tightly focused laser beam is used to send data between platforms. Because the beam is narrow, it is hard to intercept and it cannot be jammed. However, atmospheric conditions (i.e., clouds, rain etc.) can degrade or break the C2 link. ⁵⁹	In testing
Low Earth orbit communications	LEO satellite constellations provide higher bandwidth than geostationary satellites. Their lower orbital altitude reduces signal propagation distance, resulting in stronger received signals and improved resistance to jamming, although they can still be targeted. ⁶⁰ UASs can benefit from LEO-based communications, provided that they are equipped with suitable receivers and terminals capable of accessing and tracking the constellations.	Fielded
Mesh networking	Multiple platforms share data by relaying messages to one another, forming a network. If one platform is jammed, traffic reroutes through other platforms, making it difficult to disrupt the whole network. ⁶¹ In a congested EMS environment, the performance of the network can be degraded as the number of nodes grows.	Fielded
Spread-spectrum communications	The signal is spread across a wide range of frequencies, rather than broadcasting on a single channel. The signal looks like background noise; jammers cannot easily target it. The main challenge is that both the transmitter and the receiver need to synchronize their frequency patterns, which adds complexity. ⁶²	Fielded
Ultra-wideband communications	Data is transmitted in extremely short pulses spread across a very wide frequency band, which makes the signal look like background noise. This means that the signal cannot easily be detected, and therefore targeted. However, the range is limited and it works better over short distances. ⁶³	Fielded

58 Vlad Sutea, “Fiber-optic drones have emerged as critical kit for both Russia and Ukraine”, Atlantic Council, 24 February 2026, <https://www.atlanticcouncil.org/blogs/ukrainealert/fiber-optics-drones-have-emerged-as-critical-kit-for-both-russia-and-ukraine/>.

59 Tim Guest, “Battlefield potential of laser communications”, European Security and Defence, 21 September 2022, <https://euro-sd.com/2022/09/articles/technology/27182/battlefield-potential-of-laser-communications/>.

60 Jie Ma et al., “Integrated positioning and communication via LEO satellites: Opportunities and challenges”, *Arxiv*, 30 November 2024, <https://arxiv.org/html/2411.14360v2>; Ivana Kottasová, “Russia is using Starlink to make its killer drones fly farther”, CNN, 29 January 2026, <https://edition.cnn.com/2026/01/29/europe/russia-starlink-drones>.

61 Dariia Mykhailenko, “Russia builds ‘drone relay chains’ to hit Ukraine’s rear areas, defense adviser says”, United 24 Media, 28 April 2026, <https://united24media.com/latest-news/russia-builds-drone-relay-chains-to-hit-ukraines-rear-areas-defense-adviser-says-18300>.

62 Yu et al., “Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics”; Rhode & Schwarz, “Technology fundamentals: Fundamentals of hopping signals”, n.d., https://www.rohde-schwarz.com/us/knowledge-center/technology-fundamentals/hopper-signals/hopper-signals_256050.html.

63 Nikita Filippov et al., “Application of UWB technology for communication with UAVs”, 2025 IEEE 26th International Conference of Young Professionals in Electron Devices and Materials (EDM), 8 August 2025, <https://doi.org/10.1109/EDM65517.2025.11096801>.

3.2.2 Global navigation satellite system signal vulnerability

In response to the use of EW, there have also been efforts to protect GNSS signals from jamming and spoofing. Innovation efforts are focused on two broad approaches.

The first seeks to **strengthen or protect the GNSS reception** itself. This includes technologies that improve signal acquisition, resist interference, or increase the number and diversity of available navigation signals.

The second approach attempts to **reduce dependence on GNSS** altogether, through alternative navigation methods. These solutions are usually non-RF techniques and operate independently of satellite signals. Key examples include controlled reception pattern antennas (CRPAs), military PNT codes, multi-constellation receivers, signals of opportunity, LEO PNT, magnetic navigation and quantum inertial navigation systems.

These technologies are being explored across commercial and military uses (see Table 2).

TABLE 2

Innovations in position, navigation and timing

Development	Description	Development status
Controlled reception pattern antennas (CRPAs)	Blind spots are electronically placed towards the source of jamming. This allows a platform to continue receiving GNSS signals. The antennas are generally larger and heavier than standard antennas, although smaller versions are emerging. ⁶⁴	Fielded
Low Earth orbit PNT	This is derived from LEO constellations. Because LEO satellites orbit much closer to Earth, their signals are stronger than those from geostationary orbit satellites. Specialized receivers are needed to handle the rapid movement of LEO satellites. ⁶⁵	In testing
Magnetic navigation	Position is determined by measuring variations in the Earth's magnetic field and comparing them against magnetic maps. Because it does not rely on external signals, it cannot be jammed or spoofed. However, its accuracy depends on the quality of the magnetic maps. ⁶⁶	In development

64 E. Polat et al., "Design and optimization of controlled reception pattern array (CRPA) antennas for GNSS systems: Enhancing anti-jamming capabilities", 2025 Photonics & Electromagnetics Research Symposium – Spring (PIERS-Spring), 15 December 2025, <https://doi.org/10.1109/PIERS-Spring66516.2025.11276801>; Ivan Khomenko, "Iranian anti-jamming GPS found on Russian drones used in attack on Poland", United 24 Media, 13 September 2025 <https://united24media.com/latest-news/iranian-anti-jamming-gps-found-on-russian-drones-used-in-attack-on-poland-11630>.

65 Sharbel Kozhaya et al., "Unveiling Starlink for PNT", *Journal of the Institute of Navigation*, vol. 72, no. 1 (March 2025), <https://doi.org/10.33012/navi.685>; "Xona's GPS alternative draws strong US military interest", Next Gen Defence, 28 February 2025, <https://nextgendefense.com/xona-gps-alternative/>.

66 Matteo Luccio, "Riding Earth's magnetism: An alternative approach to PNT", *GPS World*, 20 July 2020, <https://www.gpsworld.com/riding-earths-magnetism-an-alternative-approach-to-pnt/>; Magnus Steena Jensen, "When GPS is jammed, we can use Earth's magnetic field", *DTU*, 15 December 2025, <https://www.dtu.dk/english/newsarchive/2025/12/when-gps-is-jammed-we-can-use-earths-magnetic-field>.

Development	Description	Development status
Military PNT codes	These modernized, encrypted GNSS signals are reserved exclusively for military users. They are far more resistant to jamming and spoofing than the civilian signal. However, specialized receivers are needed, and legacy platforms need an upgrade to access them. ⁶⁷	Fielded
Multi-constellation receivers	Rather than relying solely on one type of GNSS (e.g., either GPS, GLONASS, BeiDou), these receivers can simultaneously track signals from various systems. Using more satellite systems makes it harder to jam all signals at once. ⁶⁸	Fielded
Quantum navigation (inertial)	The properties of ultra-cold atoms are used to measure acceleration and rotation with precision. This enables a platform to calculate its position from a known starting point with accuracy that does not degrade over time, unlike conventional inertial systems. Current systems are large and require specific temperatures. Miniaturizing the technology is an unsolved engineering problem. ⁶⁹	In development
Signals of opportunity	Radio signals not originally intended for PNT (e.g., cellular, television and other commercial broadcasts) are used as opportunistic reference points for system navigation. Since these signals are ubiquitous and distributed, it is unrealistic to jam them all. ⁷⁰	In development
Terrain contour matching	Onboard radar altimeter readings are compared against pre-stored digital terrain maps to navigate. It operates entirely passively, without relying on external signals, making it resistant to jamming and spoofing. However, its effectiveness is limited over flat terrains. ⁷¹	Fielded

3.2.3 Artificial intelligence and autonomous mission execution

The integration of AI and the emergence of autonomous mission execution have become one of the most significant enabling developments shaping military systems operating in EW-affected environments. A central advantage of AI is its ability to process data collected from sensors onboard the weapon system or its components. This allows systems that use AI for support to navigate, detect threats, recognize targets and make decisions without continuous reliance on a C2 link or GNSS signals.

The integration of AI varies across applications (see Table 3). In some cases, it enhances autonomous navigation, allowing systems to operate without GNSS. In others, it improves target recognition, terminal guidance, and the detection of jamming and spoofing.

67 Brian C. Barker et al., “Overview of the GPS M code signal”, MITRE, 2000, https://www.mitre.org/sites/default/files/pdf/betz_overview.pdf ; “Galileo Public Regulated Service (PRS)”, Navipedia, European Space Agency, 16 March 2020, [https://gssc.esa.int/navipedia/index.php/Galileo_Public_Regulated_Service_\(PRS\)](https://gssc.esa.int/navipedia/index.php/Galileo_Public_Regulated_Service_(PRS)).

68 Yu et al., “Electronic warfare cyberattacks, countermeasures and modern defensive strategies of UAV avionics”.

69 Alexander M. Phillips et al., “Position fixing with cold atom gravity gradiometers”, *AVS Quantum Sci.*, vol. 4, no. 2 (June 2022), <https://doi.org/10.1116/5.0095677>.

70 Zaher M. Kassas et al., “I am not afraid of the jammer: Navigating with signals of opportunity in GPS-denied environments”, *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 7 (1 July 2022), <https://doi.org/10.1109/MAES.2022.3154110>.

71 UAV Navigation, “TERCOM-based navigation system for drones: A new era of GPS-independent flight”, Grupo Oesia, 10 September 2022, <https://www.uavnavigation.com/company/blog/tercom-based-navigation-system-drones-new-era-gps-independent-flight>.

A broader consequence of these developments is the gradual increase in operational autonomy. In some cases, cooperative behaviours between two UASs can emerge through machine learning methods. These allow systems to share information and adapt to changing battlefield conditions.

TABLE 3

Innovations in AI and autonomous mission execution

Development	Description	Development status
AI in automatic target recognition	Pattern-recognition algorithms are relied on to analyse sensor data and automatically identify and classify targets. ⁷² However, this technique requires continuous retraining and updated data to maintain accuracy in changing operational environments. ⁷³	Fielded
AI-based vision navigation	Live camera imagery is analysed by an onboard AI system to recognize landmarks and terrain features, comparing them against preloaded maps to estimate the platform's position without relying on GNSS signals. ⁷⁴ However, its performance depends on the availability of reference imagery.	Fielded
Anti-jamming classification	Genuine jamming and unintentional interference are distinguished by a software layer that listens to the EMS and uses machine learning. By identifying the jamming type of the system, it can automatically select the best countermeasure strategy. However, the AI must be regularly retrained as jamming is constantly evolving. ⁷⁵	In testing
Computer vision based terminal guidance	AI techniques are used by an onboard computer vision system to analyse sensor imagery and track a designated target during the final phase of flight. This enables autonomous trajectory corrections and allows the attack to continue even if communications are disrupted by EW. However, these systems require additional onboard processing capabilities. ⁷⁶	Fielded
Multi-agent reinforcement learning	Missions are repeatedly practised in simulation by multiple AI-controlled platforms as a cooperation training method. The result is a team of platforms that can autonomously coordinate attacks, share information and adapt. However, behaviours in simulations do not always transfer reliably to the real world. ⁷⁷	In development

72 Kateryna Bondar, *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare* (Washington, DC: Center for Strategic and International Studies, March 2025), <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>.

73 Bondar, *Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*.

74 Tereza Pultarova, "How Ukraine's killer drones are beating Russian jamming", *IEEE Spectrum*, 2 June 2025, <https://spectrum.ieee.org/ukraine-killer-drones>.

75 Raquel Delgado-Aguilera Jurado et al., "AI-driven real-time interference detection in manned-unmanned aircraft communications: Concept of operations and integration", *Aerospace Science and Technology*, vol. 168, Part A, (January 2026), <https://doi.org/10.1016/j.ast.2025.110722>.

76 Kateryna Bondar, *How Russia Is Building a Sovereign Drone Ecosystem for AI-Driven Autonomy* (Washington, DC: Center for Strategic and International Studies, April 2026), <https://www.csis.org/analysis/how-russia-building-sovereign-drone-ecosystem-ai-driven-autonomy>; Bohdan Kostiuk et al., *Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield* (Paris: Institut français des relations internationales (IFRI), February 2026), <https://www.ifri.org/en/studies/mapping-miltech-war-eight-lessons-ukraines-battlefield>.

77 Chijioke C. Ekechi et al., "A survey on UAV control with multi-agent reinforcement learning", *Drones*, vol. 9, no. (July 2025), <https://doi.org/10.3390/drones9070484>.



Space radar antenna on sunset. By zef art

4. Implications for international peace and security, arms control and disarmament

The above sections point to the importance of the EMS, and competition within it, in the military domain. They show how EW is contributing to the shaping of the deployment, operational use and design of developments in UASs and is leading to an innovation dynamic between, on one side, EW and, on the other, continued operation in EW-affected environments.

As the development and proliferation of a growing suite of UASs is one of the most important and disruptive features of modern conflicts, this dynamic is of particular relevance to international security, disarmament and arms control. This section therefore outlines key ways in which this innovation dynamic intersects with lethal autonomous weapon systems (LAWS), proliferation risks, monitoring and verification challenges, and UAS governance.

4.1 Lethal autonomous weapon systems

As discussed above, EW-affected environments create strong pressure to develop and field increasingly autonomous systems and accelerate the integration of AI-enabled functions into UASs and their operation. This has important implications for governance discussions linked to AI in the military domain and for lethal autonomous weapon systems.

More specifically, recent conflicts have demonstrated that vulnerability to EW is a key rationale (among many) driving interest in greater autonomy, particularly in systems such as UASs that operate in communications- and navigation-denied environments.⁷⁸ As described in Section 3, EW creates incentives to reduce reliance on vulnerable external links and signals altogether. This generates pressure to develop systems that are capable of independently identifying, processing, deciding and acting with reduced operator input or none at all. In practice, this means shifting certain functions (e.g., C2, GNSS, targeting) into the system itself, thereby making it more autonomous.⁷⁹

In essence, the growing prevalence of EW creates pressure to develop and field capabilities that are associated with LAWS.⁸⁰ While EW is not the only pressure or variable that is driving adoption of autonomy, and many remaining problems impede fielding highly autonomous capabilities, EW contributes by exacerbating the perceived need for such capabilities. By shaping the operational environment in which capabilities are deployed, EW can therefore be considered as being partly responsible for decisions to increase autonomous capabilities in weapon systems such as UASs. This has a direct impact on ongoing arms control discussions linked to LAWS. Indeed, this dynamic creates an inherent tension: the multilateral discussions, including in the GGE on LAWS under the Convention on Certain Conventional Weapons (CCW), have broadly focused on a combination of prohibitions and regulations. But these discussions are taking place against the backdrop of operational demands for full autonomy, including in EW-affected environments.⁸¹

Furthermore, increasingly contested electromagnetic environments entail that efforts to maintain and preserve human control or oversight over capabilities while those capabilities are in operation may not always be technically feasible or aligned with operational realities. The 2026 consensus report of the GGE on LAWS stressed that human beings exercise control “directly or indirectly, including through measures taken before and/or during the use of LAWS”.⁸² In highly contested EMS environments

78 Bondar, *Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare*.

79 Vitaly Goncharuk, “Chasing true AI autonomy: From legacy mindsets to battlefield dominance”, War on the Rocks, 15 December 2025, <https://warontherocks.com/chasing-true-ai-autonomy-from-legacy-mindsets-to-battlefield-dominance/>.

80 While no universally agreed upon definition of LAWS exists, they may be characterized as in the report of the 2024–2026 sessions of the GGE on LAWS “as a combination of one or more weapons and technological components operating together, that is capable of identifying, selecting, and engaging a target in a way that results in loss of life, without intervention by a human being operating the system”. Convention on Certain Conventional Weapons, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems, Report of the 2024–2026 sessions, CCW/GGE.1/2026/3, 14 September 2026, <https://docs.un.org/CCW/GGE.1/2026/3>, paragraph 25.

81 Eric Rosenbach, Ethan Lee and Bethany Russell, *The Autonomous Arsenal in Defence of Taiwan: Technology, Law and Policy of the Replicator Initiative* (Cambridge, MA: Harvard Belfer Center for Science and International Affairs, January 2025), [https://www.belfercenter.org/sites/default/files/2025-02/DETS_The Autonomous Arsenal_1.pdf](https://www.belfercenter.org/sites/default/files/2025-02/DETS_The%20Autonomous%20Arsenal_1.pdf).

82 Convention on Certain Conventional Weapons, CCW/GGE.1/2026/3, paragraph 34.

where direct oversight may no longer be possible, the operational realities increase the importance of upfront measures (i.e., measures taken before the operation of LAWS) to ensure compliance with international humanitarian law (IHL). However, those realities may simultaneously reduce the possibility of ensuring IHL compliance solely to those upfront measures.

Discussions on LAWS at the multilateral level should therefore pay close attention to developments in EW as EW will continue to shape the rationale and the means for integrating AI-enabled autonomy in UASs (and weapon systems more broadly), as well as the environments in which LAWS operate.

4.2 Proliferation risks

The dual-use nature of the technologies that enable EW, as well as the countermeasures and related innovations in weapon systems, raises proliferation concerns. These are chiefly related to the proliferation of disruptive EW capabilities and EW countermeasures to new States and to non-State actors.

As noted throughout this primer, the technologies that enable access to the EMS, as well as those used to disrupt access and those developed as countermeasures to disruption, are dual-use. For example, spread-spectrum communications are commonly embedded in WiFi and Bluetooth technologies; ultra-wideband technologies are integrated into smartphones and consumer electronics; beamformed communications are used in 5G and advanced WiFi systems; and mesh networking capabilities are increasingly common in commercial networking equipment. While this is a familiar issue for technology-related governance, it is one worth taking note of in the context of EW and the potential global consequences of the proliferation of these technologies as enablers of growing interference.⁸³

Indeed, the dual-use nature of these technologies may help proliferate to non-State actors both the capabilities to interfere with the spectrum as well as those meant as countermeasures to allow operation in EW-affected environments. For example, while the development and fielding of fibre-optic UASs was primarily driven by inter-State conflicts, recent interest in, and use of, fibre-optic UASs by non-State armed groups illustrates the broader appeal – and ease of proliferation – of EW-resistant capabilities in UASs.⁸⁴ The expanded ability of non-State and malicious actors to both operate in EW-affected environments and to affect the spectrum could foster greater instability. For example, increasingly survivable platforms will foster the development and proliferation of increasingly powerful EW capabilities and reinforce an existing trend for growing use and impact of EW globally.⁸⁵

83 Elizabeth Braw, “The Epidemic of GPS Jamming”, *Foreign Policy*, 1 June 2026, <https://foreignpolicy.com/2026/06/01/gps-jamming-hormuz-russia-baltic-aviation-shipping-trade>; Zak Kassas, “From Hormuz to the cockpit: How warfare and criminal activity undermine GPS and the race to safeguard navigation”, *The Conversation*, 23 June 2026, <https://theconversation.com/from-hormuz-to-the-cockpit-how-warfare-and-criminal-activity-undermine-gps-and-the-race-to-safeguard-navigation-281106>.

84 Vlad Sutea, “Fiber-optic drones have emerged as critical kit for both Russia and Ukraine”, *Atlantic Council*, 24 February 2026, <https://www.atlanticcouncil.org/blogs/ukrainealert/fiber-optics-drones-have-emerged-as-critical-kit-for-both-russia-and-ukraine/>; “Fiber optic FPV drones emerge on African battlefields”, *Military Africa*, 29 August 2025, <https://www.military.africa/2025/08/fiber-optic-fpv-drones-emerge-on-african-battlefields/>; Lucy Williamson, “Learning from Ukraine war, Hezbollah is now using fibre-optic drones to hit Israel”, *BBC*, 28 May 2026, <https://www.bbc.com/news/articles/c0r2ydlvk41o>.

85 GPS Spoofing Working Group, “GPS spoofing”, Final report, OPS Group, 6 September 2024, <https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf>.

Relatedly, EW may contribute to driving the development and proliferation of other types of conventional military equipment used as countermeasures to UASs.⁸⁶ Indeed, as UASs become increasingly resilient to EW, this may drive the need for – and innovation in – physical counter-UAS measures.⁸⁷ For example, renewed emphasis has been put on small-calibre air defence guns and directed energy weapons (DEWs).⁸⁸ This could also lead to the need for further discussions on governance of weapon technologies, such as DEWs, that may form part of the counter-UAS trend but currently are not directly encompassed by counter-proliferation or arms trade regulation mechanisms. It is important to note, however, that EW is not the only driver of this trend. Other drivers include the overall numerical increase of UASs in modern battlefields and the cost imbalance between UASs and the traditional means to intercept them.⁸⁹

4.3 Monitoring and verification challenges

To avoid a “race to the bottom” in deploying systems, the ability to monitor and assess capabilities becomes particularly important. However, the pace of innovation in this space and the dual-use nature of the relevant technologies complicates monitoring efforts. Moreover, a defining feature of many EW countermeasures is their reliance on software-defined architectures, which allow systems to be updated, reconfigured or enhanced without hardware changes. Technologies such as spread-spectrum communications, beamforming, mesh networking and AI-driven signal processing can all be adapted through software updates, enabling rapid responses to evolving threats. While this flexibility enhances adaptability and cost-efficiency, it also impedes transparency and observability.

In addition, the innovation cycle between UASs and their countermeasures is accelerating.⁹⁰ The speed of innovation required by the contest in this domain may create competitive pressures to develop and field capabilities and countermeasures increasingly quickly. Because capabilities can be modified quickly and often without visible changes to hardware, it becomes more difficult to track, assess and verify system capabilities over time.⁹¹ The pace at which software can evolve raises the possibility that capabilities may expand significantly, without clear external indicators. This would complicate efforts to monitor technological developments and evaluate their implications.⁹²

86 Zachary Kallenborn and Marcel Plichta. “Drone, counterdrone, counter-counterdrone: Winning the unmanned platform innovation cycle.” Modern War Institute, West Point, 23 September 2024, <https://mwi.westpoint.edu/drone-counterdrone-counter-counterdrone-winning-the-unmanned-platform-innovation-cycle/>; UNIDIR, “Directed energy weapon developments in counter-UAS defence”, 24 June 2026, <https://unidir.org/event/directed-energy-weapon-developments-in-counter-uas-defence/>.

87 Kallenborn and Plichta. “Drone, counterdrone, counter-counterdrone”.

88 Interview with Thomas Withington; Kallenborn and Plichta. “Drone, counterdrone, counter-counterdrone”; Alex Carter, “Fiber-optic drones: The unjammable weapons changing modern warfare”, Military Machine, 5 March 2026, <https://militarymachine.com/fiber-optic-drones-unjammable-weapons>.

89 UNIDIR, “Directed energy weapon developments in counter-UAS defence”.

90 Kallenborn and Plichta. “Drone, counterdrone, counter-counterdrone”.

91 Interview with Ioannis Vagias.

92 Artem Sherbinin and Austin Gray, “Software-defined warships: The navy’s digital future of necessity”, War on the Rocks, 10 February 2025, <https://warontherocks.com/software-defined-warships-the-navys-digital-future-of-necessity/>.

4.4 UAS governance

Because electronic warfare drives adaptations in UASs, affects their path of development and influences their operational use, this makes EW directly relevant to disarmament and arms control discussions linked to UASs and to uncrewed systems more broadly. Arms control efforts linked to UASs are chiefly concerned with the tracking of the transfer of systems and their components.⁹³ However, it is important for the international community to remain abreast of qualitative developments in this field and recognize their importance. Indeed, this EW-driven cycle of innovation will continue to influence what types of UAS proliferate, why they proliferate and, importantly, also how their evolving characteristics affect their risk profile. For example, the proliferation of technologies that enable operation within an EW-affected environment raises questions about how to ensure the continued suitability of defences against threats linked to UASs.⁹⁴

It would be beneficial to further unpack whether EW-resistant UASs are qualitatively different in a way that makes them riskier in the context of non-State actor use (e.g., as platforms for delivery of weapons of mass destruction) as well as use by States, and would therefore warrant specific governance attention. This may require the international community to consider how the evolution of UASs in the context of EW affects key governance efforts relevant for their export, transfer and use such as United Nations Security Council resolutions 2370 (2017) and 1540 (2004), as well as the Arms Trade Treaty.

93 Grand-Clément, “Armed and dangerous?”.

94 Max Hunder, “Russia evades Ukraine electrical substation defences with small, unjammable drones”, Reuters, 10 July 2026, <https://www.reuters.com/business/aerospace-defense/russia-evades-ukraine-electrical-substation-defences-with-small-unjammable-2026-07-10/>.

5. Conclusion

Electronic warfare has become a central feature of contemporary military competition, reflecting the increasing dependence of modern weapon systems on the electromagnetic spectrum. As this primer shows, the same functions that enable advanced military capabilities in communications, sensing, navigation and guidance also create systemic vulnerabilities. Jamming and spoofing exploit these vulnerabilities by disrupting or manipulating signals, thereby degrading or denying the performance of weapon systems without causing physical destruction. As seen, UASs are particularly vulnerable to EW, as it consistently targets the critical radio-based links that underpin core functions such as command and control, satellite navigation and radar-based tracking. Disruption of the EMS used by these systems creates operational uncertainty, leading to reduced accuracy and, in some cases, loss of control. It is in this context that EW has become a driver of innovation in UASs and their countermeasures.

Militaries are developing a wide range of technologies to increase the resistance of UASs. These include efforts to strengthen GNSS reliability through anti-jamming and anti-spoofing measures, while simultaneously reducing reliance on radio frequency-based position, navigation and timing by incorporating complementary non-RF methods. Communications are being reinforced through anti-jamming measures and low-probability-of-detection techniques to protect the C2 link from interference. In addition, sensing is increasingly turning to low-probability-of-detection techniques. Finally, emerging technologies, such as AI, are enabling systems to operate in EW-affected environments by enhancing signal processing, adaptability and decision-making. These measures are often layered to provide redundancy, reflecting an understanding that no single solution can fully mitigate EW threats. Applied together, they are leading to the accelerated development of systems that are capable of operating with reduced, minimal or no dependence on continuous external inputs.

EW-driven innovation dynamics carry with them multiple governance challenges for international security, disarmament and arms control.

First, pressures to increase autonomy, driven by the need to operate in EW-affected environments, raise concerns within ongoing discussions on LAWS. This is particularly the case regarding the pressure to develop and field weapon systems with increased autonomy to match increasingly powerful EW developments, complicating considerations surrounding human control over systems operating in increasingly electromagnetically contested environments.

Second, the measure-countermeasure dynamic between EW and UASs can accelerate the proliferation of disruptive EW capabilities and their countermeasures, especially to non-State actors. This is further exacerbated and complicated by the dual-use nature of the relevant technologies.

Third, while these trends emphasize the necessity for monitoring and verification of capabilities, the specificities of EW-related technologies – their software-defined nature and the pace of innovation – make this particularly difficult.

Lastly, the dynamics outlined in this primer raise questions for governance efforts linked to the use and export of UASs. This requires that more discussions focus on EW-driven qualitative developments in

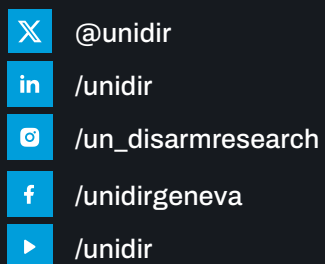
UASs, and how these affect these systems' risk profile. More awareness may provide the international community with a clearer picture of the direction of development of UASs and therefore what specific types – and with what level of capability – may proliferate.

Overall, the findings suggest that EW should be understood not only as a battlefield activity but as a strategic force that is shaping the development trajectory of weapon systems. For the disarmament and arms control community, this underscores the need for more systematic engagement with EW, its associated innovation pathways, its impact on weapon systems and its significance for existing governance frameworks. Greater conceptual clarity, sustained dialogue between technical and policy communities, and improved monitoring of emerging technologies will be essential to ensure that evolving EW or related practices do not outpace international security and arms control efforts.

Appendix A. List of interviewees

We are grateful for the following experts who took part in the research interviews and for the information they contributed.

Name	Affiliation	Date of Interview
Mr. Ioannis Vagias	Cranfield University	10 February 2026
Ms. Clémence Poirier	ETH Zurich	12 February 2026
Dr. Thomas Withington	Royal United Services Institute and NATO Defence College	18 February 2026
Mr. Ruben Stewart	International Institute for Strategic Studies	19 February 2026
Prof. Warren du Plessis	University of Pretoria	24 February 2026
Anonymous interviewee	Royal Institute of Navigation	25 February 2026
Mr. Zachary Kallenborn	King's College London	6 March 2026
Dr. Ivan Zaccagnini	ETH Zurich	12 March 2026
Dr. Marc De Vore	University of St Andrews	17 March 2026
Mr. James Black	RAND Europe	18 March 2026
Prof. Mireille Elhajj	Imperial College London	7 April 2026
Dr. Gregory Falco	Cornell University	10 April 2026
Mr. Duncan McCrory	King's College London	13 April 2026
Prof. Andrew J. Futter	University of Leicester	27 April 2026
Dr. Ana Sánchez Coboleda	University of Barcelona	30 April 2026



Palais des Nations
1211 Geneva, Switzerland

© 2026, UNIDIR

UNIDIR.ORG