Journal of the Spanish Institute for Strategic Studies
ISSN-e: 2255-3479

Tania Vidal López
PhD in Law, Political Science and Criminology from the University of Valencia.

Email: taniavidallopezphd@gmail.com

Technology and armed conflict: the transformation of war in the 21st century

Abstract

In recent decades, warfare has undergone a profound transformation driven by digitalisation and rapid technological development. These advances have not only altered the operational capabilities of states, but have also changed the global dynamics of security and defence. Technology has redefined the theatre of war, giving rise to conflicts that transcend conventional means and demand a reconfiguration of military tactical and operational strategies. In this context, the concept of hybrid warfare has emerged, characterised by the combination of traditional and unconventional tactics, including cyber operations, disinformation and attacks on critical infrastructure. This new paradigm seeks to exploit systemic vulnerabilities and destabilise states without necessarily resorting to direct confrontation. As a result, cybersecurity and cyber defence have become essential pillars of contemporary defence policies. International institutions, such as the European Union, have recognised the urgency of strengthening their resilience in the face of these emerging threats, developing comprehensive strategies that integrate technology, intelligence and international cooperation to protect global stability and security. In short, the digital age has redefined the very nature of warfare and international security.

Keywords

Hybrid threats, Defence, National Security Strategy, European Union, Grey zone.

Cite this article:

Vidal López, T. (2026). Technology and armed conflict: The transformation of war in the 21st century. *Journal of the Spanish Institute for Strategic Studies*. 27, pp. 251–270.

1 Introduction

In recent decades, we have witnessed a profound transformation in the way war is conceived and waged, driven mainly by digitalisation and rapid technological advancement and development. This evolution has not only altered countries' operational capabilities but has also led to a significant shift in global security and defence dynamics.

In an increasingly multipolar and competitive international context, new actors—both state and non-state—have emerged, employing novel and innovative unconventional mechanisms and tools capable of disrupting the *status quo* and destabilising the foundations of modern societies. This phenomenon undoubtedly has a direct impact on the defence and security sphere, leading to a reconfiguration of military tactical and operational strategies and generating new forms of conflict that go beyond conventional means.

One of the most obvious manifestations of this evolution and transformation in the way war is waged is the emergence of a new arena in these conflicts: cyberspace. Far from being confined to traditional battlefields, modern conflicts are now also taking place in the digital realm, with the advent of cyberspace and the use of emerging technologies. Consequently, the cyber domain has become a key element of armed conflict, with the capacity to destabilise, influence or undermine a country's critical infrastructure or information systems, as we are witnessing in Russia's war of aggression against Ukraine. This reality has led to the modernisation of conflict and the transformation of a country's defence strategy and organisation, characterised not only by conventional military tactics but also by the inclusion of digital mechanisms and tools.

This new paradigm of armed conflict falls within the concept of *hybrid warfare* (HW), which combines numerous techniques and methods with the aim of exploiting a country's potential systemic vulnerabilities. At the heart of this new form of warfare lies the cyberspace arena, which has taken on a prominent role in recent years, where the identification and attribution of actions is particularly challenging. In this scenario, traditional military strategies are combined with new technological mechanisms, giving rise to the modernisation of conflict and the so-called HW; consequently, the actual response capacity of international institutions, in particular the European Union (EU) and the North Atlantic Treaty Organisation (NATO), in the face of hybrid threats that combine military action, information warfare and cyberattacks

Therefore, this article begins with a specific research question: to what extent has the war in Ukraine altered the understanding and design of European defence against hybrid threats and cyberattacks? Based on this question, it is argued that the conflict has revealed both the strategic value of technology and the limits of the institutional responses of the EU and NATO. The significance of the Ukrainian case lies not only in its military dimension, but in its ability to demonstrate how the combination of cyberattacks, disinformation, electronic warfare and technological innovation alters the traditional logic of conflict and forces a rethinking of defence frameworks.

2 Methodology

This study adopts a qualitative documentary analysis approach based on institutional, strategic and academic sources. The corpus analysed includes EU security and cybersecurity strategies, NATO strategic documents, specialist reports and recent literature on hybrid warfare, disinformation, military innovation and the Russian-Ukrainian conflict.

In this vein, the study is structured as an illustrative case study centred on Ukraine, used to draw broader implications regarding the contemporary transformation of warfare and the adaptation of European defence. To this end, the analysis is organised into four main dimensions: cyberspace, disinformation, technological innovation and the institutional response. This approach allows for a comparison of the strategic discourse of the EU and NATO with the empirical evidence from the conflict and identifies gaps between normative ambition and operational capability.

The selection of documents was based on their strategic relevance, topicality and direct relationship to the subject of study.

3 Defence in cyberspace

It is important to note that, in Spain, both the 2018 National Security Strategy and the 2019 National Cybersecurity Strategy have warned of the rise of so-called hybrid threats. Based on these documents, hybrid threats should be understood as deliberate actions aimed at exploiting the systemic vulnerabilities of a democratic state and its institutions, through the use of a variety of methods, including conventional military operations, disinformation campaigns or cyberattacks.

The EU has promoted various measures and initiatives to strengthen its capabilities against cyber threats; however, the crucial issue is not merely the existence of these instruments, but their actual degree of coordination, implementation and operational effectiveness in the face of complex and persistent attacks.

Among these, it is worth highlighting the proposal for a common cybersecurity certification framework, the modernisation of the EU's Cybersecurity Agency (ENISA), as well as the promotion of cooperation between Member States and EU agencies in the event of cyberattacks. In this context, we also see the development of a specific training and education platform with the primary aim of enhancing collaboration on joint cyber defence efforts.

In fact, in 2020, the European Commission, together with the European External Action Service (EEAS), unveiled a new Cybersecurity Strategy for the EU. The main purpose of this new strategy is to strengthen Europe's resilience in the face of growing cyber threats. The proposal includes specific proposals, which are geared towards the implementation of regulatory, operational and investment measures.

Subsequently, in 2021, the Council of the EU adopted conclusions on this cybersecurity strategy, emphasising that cybersecurity is an essential and indispensable element in ensuring a resilient, digital and sustainable Europe. Within this framework,

EU ministers established as a priority the achievement of strategic autonomy without compromising other aspects such as the economy, thereby enabling them to strengthen digital leadership and, consequently, increase their strategic capacity in the field of cybersecurity.

With all this in mind, we observe that the development of resilience against hostile actions in cyberspace depends to a large extent on coordination between actors, in this case between the Member States and other international organisations, with particular emphasis on cooperation with NATO.

In this context, NATO set out a strategy as early as 2015 to combat hybrid threats, focusing its efforts on both political and military adaptation. These initiatives were discussed and received a favourable response, culminating in various agreements following the 2016 Warsaw Summit, which regarded hybrid warfare as a real threat against which deterrence mechanisms must be strengthened, whilst promoting preparedness and defence (Gutiérrez, 2021). We can therefore state that it was NATO that began to lay the foundations for countering hostile actions carried out in cyberspace, which have great potential to damage and undermine the integrity of a state.

At the summit held in Madrid in 2022, the issue of hybrid threats was addressed once again, prompted by Russia's war of aggression against Ukraine, where the strategic potential of hybrid threats is evident even in a context of armed conflict, with the consequent Russian threat to Euro-Atlantic stability.

In short, in the face of this unstable context, the EU and NATO are charting a course towards strategic autonomy, guided by two key documents: firstly, the Strategic Compass, which is an action plan for 2030, and secondly, the Atlantic Alliance's New Strategic Concept. Both instruments address current challenges and commit to a more robust and coordinated common defence.

At this point, one of the main tensions within the European framework emerges: regulatory progress does not always translate into a uniform response capacity among Member States.

4 The grey zone strategy

Conflicts within the grey zone (GZ) represent one of the most characteristic forms of contemporary confrontation, precisely because they allow strategic objectives to be achieved without the need to unleash open warfare (Gutiérrez, 2021). This reality has numerous implications for the planning and execution of military operations at all levels of the conflict. Its analytical value lies in the fact that it effectively explains the ambiguity, gradual nature and difficulty of attribution that characterise many of today's hybrid operations.

The first consensus-based approach to this concept is framed *in the negative*, that is, as the use of attitudes and instruments that are neither 'white' like peace, nor 'black' like open warfare, whether hybrid or conventional. In other words, it is an

intermediate scenario referred to as 'grey', which can be considered a *sui generis* variant of hybrid warfare (Baqués, 2017).

We therefore speak of GZ when the scenario of hostile activities does not involve direct armed confrontation, but rather the use of mechanisms with sufficient destructive potential to destabilise a country, such as disinformation tactics, the use of hybrid threats or cyberattacks. These actions, which do not involve physical violence, are becoming increasingly frequent, although it cannot be ruled out that these hostile operations and their development over time may ultimately escalate into an armed conflict.

GZ strategies are carried out with the aim of achieving a similar objective to that of initiating an armed conflict; in short, this strategy relies on technological evolution acting as a multiplier, yet without crossing the threshold that would justify a traditional military response. The effectiveness of these tactics, therefore, lies in their capacity to cause harm, coupled with the difficulty of detection, attribution and a timely response.

In fact, the *Multinational Capability Development Campaign* (MCDC) states that actors employing these strategies do so in a coordinated manner using various instruments of power, which are tailored to exploit the specific vulnerabilities of the target country.

The purpose of GZ actions is to carry out initiatives designed to be executed without being detected, going unnoticed and/or not justifying a military reaction due to their low profile, yet which nevertheless have the potential to cause significant real-world effects. Indeed, on occasions, even when the attack is identified, it is difficult to attribute responsibility for it.

In any case, when an actor opts to employ the GZ strategy, they are aware that results will not be achieved immediately, but rather that this is a long-term goal, where the concept of 'strategic gradualism' may be invoked, even serving as a precursor to open warfare (Baqués, 2017).

For all these reasons, it is clear that among the main challenges of defence in the GZ are the lack of clarity regarding the nature of the conflict, the difficulty in precisely identifying the parties involved, as well as the uncertainty surrounding the application of relevant public policies or legal frameworks (Silva, 2022). Thus, the role of the cognitive environment is fundamental to this strategy, as social and international perceptions can influence the situation; consequently, it is necessary to control information in order to achieve superiority in this domain (Gutiérrez, 2021). It follows that, in order to respond effectively to these threats within the GZ environment, it is essential to have centralised and coordinated planning, as well as resilient structures and a strategic vision for the armed forces that enables the early and effectiv tion of and response to such attacks.

However, the concept of the GZ also has explanatory limitations when applied to high-intensity conflicts, where hybrid operations coexist with large-scale conventional attacks.

5 The new paradigm of warfare

The rapid advancement of technologies, converging with an increasingly digitalised world, has brought about profound transformations in all areas of society, as well as in the field of defence and security (Rodríguez, *et al.*, 2023). This technological evolution as a transformative factor has led to the inclusion of new digital tools such as autonomous systems, artificial intelligence (AI), predictive analytics and cybersecurity, amongst others, which directly affect the security and defence sector, redefining not only existing threats but also the strategies and capabilities required to counter them.

In this context, these emerging technologies have come to play a central role in shaping states' strategic capabilities, as well as in the conduct of warfare; examples of this include the use of cyberattacks, armed drones, or AI itself applied to intelligence analysis and military operations, which illustrate how contemporary conflicts are fought in increasingly complex and digitised scenarios, generating a paradigm shift in which technological superiority can be a decisive factor on the battlefield.

That is to say, technological advancement not only transforms the tools available to ensure a state's security and defence but, in parallel, also entails the need to rethink organisational and regulatory frameworks to ensure optimal capabilities for managing these new environments, requiring a clear multidisciplinary approach.

This rapid technological progress has substantially altered the understanding of armed conflicts, giving rise to the concept of HW, a term widely adopted by the international defence community (Franco, 2023), to describe a situation of confrontation that combines elements of conventional warfare with the new tools of the cyber domain. In other words, it helps us understand how technology expands and diversifies the instruments of coercion available to state and non-state actors.

Unlike traditional armed conflicts, which unfold primarily in a physical theatre through direct military operations, HW integrates multiple dimensions, including military, political, informational and cyber. Thus, alongside traditional actions, tactics such as cyberattacks or disinformation are deployed to destabilise the adversary without resorting exclusively to the explicit use of force.

Consequently, the use of these new technologies leads to a paradigm shift in the nature of war, where physical boundaries become blurred. HW typically unfolds in a complex environment involving actors employing more sophisticated techniques, where it can be difficult to attribute responsibility for actions, and where, as a result, more traditional legal and strategic responses are often insufficient.

This implies that contemporary warfare can no longer be analysed solely from the perspective of kinetic conflict, but also from the capacity to influence information systems, digital networks, public perception and institutional resilience.

Consequently, this transformation poses significant challenges for International Humanitarian Law, as well as for Public International Law in general. An example of this is the case of Russia's war of aggression against Ukraine, which represents a

paradigmatic case for reflecting on the key role played by technologies in shaping and developing contemporary warfare.

Therefore, the Ukrainian case not only illustrates the technological transformation of warfare, but also the need to rethink the doctrinal, legal and strategic frameworks through which armed conflict is interpreted.

Beyond the geopolitical and humanitarian dimensions of the conflict, Ukrainian territory has become a veritable theatre of operations where new forms of warfare are being tested and refined, based on the primary—and indeed central—use of the digital tools and mechanisms provided by emerging technologies.

This conflict has highlighted how new technologies have been integrated into military strategy alongside traditional strategies, acquiring significant relevance, ranging from attacks on critical infrastructure to the dissemination of disinformation campaigns and the manipulation of public opinion on a global scale.

This reality makes Ukraine not only a theatre of armed conflict, but also a technological laboratory for innovation in security and defence, where various actors—both state and non-state—are testing emerging technologies in the real-world context of war. This situation raises numerous fundamental questions regarding the ethics and use of technologies, as well as their regulation and long-term consequences when applied to such highly hostile scenarios and, in particular, with a view to future conflicts.

In short, it is worth emphasising that, in this context—as is the case in Ukraine—it is clearly illustrated how 21st-century warfare has ceased to be a phenomenon confined exclusively to the physical battlefield, becoming instead a complex, multidimensional scenario where technological supremacy can be an indicator of effective resilience in the face of conflict.

6 Defence Innovation: A Reflection of Russia's War of Aggression Against Ukraine

The digital transformation currently sweeping the contemporary world, as we have seen, has had a direct impact on the security and defence sectors, altering traditional ways of conceiving, planning and executing armed conflicts.

In this new scenario, war is no longer limited territorially on the physical plane, but extends into the realms of cyberspace, information and technological dominance. And the conflict between Russia and Ukraine, as a concrete expression of this change, allows us to clearly observe how technology has positioned itself as a key element in the development of the armed conflict between these countries.

This confrontation reflects how armed conflicts are capable of effectively combining traditional weaponry with disruptive emerging technologies. Both countries have resorted to conventional means, such as armoured vehicles or heavy artillery, whilst simultaneously integrating innovative technologies, such as unmanned vehicles, AI systems, coordinated cyberattacks and advanced digital surveillance tools. This fusion

of tactics clearly demonstrates the hybrid nature of current conflicts and highlights the transformation of military strategy at a global level.

In this vein, the statements made at the start of the conflict by Mykhailo Fedorov, Ukraine's Deputy Prime Minister and Minister for Digital Transformation, via his social media channels, reveal a vision that highlights the crucial role of new technologies. In these statements, he asserted that the country's future victory would depend not only on the courage of the population, but on the strategic use of new technologies. These remarks are not merely a political message, but a statement of principle regarding the role that technological advances play in modern warfare, where superiority no longer depends solely on troop numbers or conventional weaponry, but on the ability to integrate information, technology and command under conditions of high uncertainty.

Ukraine has succeeded in significantly enhancing both its defensive and offensive capabilities through the use and integration of technologies on the battlefield, making its experience a relevant case study , particularly for Europe. This conflict has highlighted the fundamental role played by technology and innovation in the defence sector, demonstrating rapid adaptation to the new landscape of modern warfare. This profound transformation in the way war is waged has therefore altered the structure and operations of armed forces. In this context, the Ukrainians' experience of the conflict offers valuable lessons on how to optimise response capabilities, including resources and means, through the integration of emerging technologies—such as drones, AI, electronic warfare, etc.—in a high-intensity conflict. This is key to strengthening national security and redefining the collective defence strategy at the European level.

Indeed, Ukraine has demonstrated a remarkable capacity for technological adaptation throughout the conflict, drawing further on direct collaboration with leading Western high-tech companies such as Palantir, Clearview AI, Delta and GIS ARTA, amongst others. Undoubtedly, these public-private partnerships have facilitated the use of advanced technology-based solutions, which have been crucial at certain moments from a military intelligence perspective, effectively contributing to tactical and operational strategy on the battlefield. This technological ecosystem has provided Ukraine with a significant adaptive advantage based on rapid response capability.

For example, Palantir is software that enables information superiority; that is, it has allowed Ukrainian forces to obtain real-time data analysis, which has facilitated a marked improvement in decision-making, acting as a force multiplier that has increased the military's effectiveness and combat potential. Meanwhile, Clearview AI has provided advanced capabilities for the reconnaissance and identification of combatants. For its part, Delta is software that enables real-time mapping of the front line's progress. Consequently, this programme has enabled the efficient coordination of military units, even in volatile environments, thanks to international support. As for GIS ARTA, it is a system that integrates AI with satellite internet, which has optimised the response of Ukrainian artillery capabilities, facilitating attacks on enemy positions with greater immediacy and effectiveness.

These tools should not be interpreted as isolated solutions, but as part of a technological adaptation ecosystem that combines intelligence, mobility, coordination and real-time responsiveness.

With regard to Europe's analysis of the conflict, it is important to note that the European Commission has launched various initiatives, such as the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO), which reflect a commitment to strengthening joint military capabilities and fostering technological innovation in the field of common defence. These tools aim to consolidate a comprehensive technological foundation in the field of security and defence that is more efficient amongst the Member States, with a focus on promoting collaborative projects in key areas such as AI and cybersecurity. For all these reasons, the analysis of Russia's war of aggression takes on strategic importance, as practical lessons can be drawn from its study regarding the adaptation of European military strategy to current challenges, where technology plays a central role in operational effectiveness and resilience against hybrid and conventional threats.

However, this transformation is not without controversy. The use of these new technologies in wartime contexts raises significant ethical, legal and geostrategic challenges, including the difficulty of proving the authorship of certain cyber actions and, consequently, the complexity of establishing and attributing responsibility for them. In addition to the implications for military strategy, which span multiple dimensions, from tactical and logistical planning to intelligence, cyber defence, and the management of the territory itself.

Furthermore, this transformation also introduces strategic dependencies, particularly with regard to external technology providers, digital supply chains, and capabilities for ongoing maintenance and updating.

6.1 Disinformation

Disinformation techniques have been amplified by the use of Information and Communication Technologies (ICT), which have been employed as a vehicle to rapidly transmit and disseminate information, bypassing geographical barriers and highlighting the potential and capacity of ICT to reach an indeterminate number of people efficiently and effectively.

ICT has revolutionised the way information is created, disseminated and consumed globally. Its ability to amplify messages in real time and reach a large number of individuals has significantly increased its influence on public opinion, not only at the national level but also internationally. Consequently, this transformation in communication has given rise to a broader information landscape that is highly accessible, which also allows social perceptions to be deliberately shaped.

In this context, state and non-state actors have exploited ICTs to develop highly effective disinformation campaigns, which not only distort the facts but also seek to erode trust in institutions, delegitimise them, polarise international society and generate confusion at critical moments such as during a war (Alastuey *et al.*, 2024).

The mechanisms typically employed in these disinformation campaigns are based on the distorted dissemination of reality using false data, misrepresenting it, or directly manipulating it. The ease with which this information—which directly affects public opinion—can be manipulated poses a latent challenge, as these disinformation campaigns undermine information security and, consequently, overall security; indeed, our National Security Strategy (ESN21) identifies this tactic as a serious threat to national security.

In the Russian war of aggression, these campaigns have been used for propaganda purposes, with the aim of reaching both those affected and potential supporters of the armed conflict.

Typically, these disinformation campaigns used for propaganda are designed to undermine the adversary's morale and extol one's own strengths. Similarly, the use of multiple information sources, such as traditional media or even social media, has established itself as an ideal vehicle for carrying out these disinformation actions. Tools such as *fake news* illustrate how these channels can be exploited to delegitimise the adversary's actions and, at the same time, justify one's own, in a clear attempt to manipulate public perception and shape international opinion.

These communication tools not only seek to confuse or deceive, but their primary aim is to shape the dominant narrative of the conflict, influencing key actors in the international community and consequently generating global division. All in all, disinformation is yet another weapon in the arsenal of tactics employed by a state within the HW, with a significant impact and devastating potential on legitimacy and social cohesion, as well as the ability to potentially disrupt the decision-making processes of the international community.

The fight against disinformation is a complex challenge that requires a combined and coordinated response. In this regard, it is worth noting that Spain has developed a comprehensive and robust legal and operational framework, involving government institutions and social actors (Alastuey *et al.*, 2024). However, the effectiveness of this approach is not static but depends on the ability to adapt to the evolution of new technologies. In this regard, it is essential to emphasise that to combat disinformation effectively, civil-military engagement must be strengthened to reinforce communication systems and ensure the greatest possible transparency, particularly with the media.

At the international level, collaboration with the EU and NATO is essential to bolster states' capabilities and provide an effective response to these threats that transcend borders and undermine global stability. These alliances enable the sharing of knowledge and the coordination of efforts, whilst demonstrating a global and proactive commitment to addressing these hybrid threats. Only a comprehensive approach, based on education, transparency and collaboration, can contribute to a society that is more resilient in the face of the challenges posed by contemporary disinformation.

In this regard, disinformation should not be understood as a secondary phenomenon, but as a structural instrument of HW, whose effectiveness depends both

on the sender's capacity to produce manipulated content and on the vulnerability of the information ecosystem in which such content circulates.

6.2 Cyberspace

Cyberspace, virtually unexplored in the armed conflicts of the 20th century, has become a central strategic arena in the modern wars of the 21st century, as evidenced both in the conflict between Russia and Ukraine and in other recent cyberattacks linked to the escalation in Gaza.

In the case of Ukraine, from the very first days of the invasion, Russia launched a series of cyberattacks targeting the Ukrainian state's critical infrastructure, in an attempt to destabilise its institutional and logistical capabilities. Among these cyberattacks, one stands out: the denial-of-service (DoS) attack carried out against the country's main telecommunications company, *Ukrtelecom*. Through this attack, Russia succeeded in disrupting communications, leaving large swathes of the population cut off for several hours (SSSCIPU, 2022).

This case illustrates that cyberspace does not function as a domain separate from warfare, but rather as a force multiplier capable of disrupting logistics, morale and institutional continuity.

Nevertheless, Ukraine has managed to mount a relatively effective digital defence which, despite the asymmetry of resources, has made it possible to contain, neutralise and even reverse some of the hostile operations. In other words, Ukraine responded with a combination of digital resilience, cooperation with Western allies and support from technology companies, which enabled it to maintain institutional operations and strengthen the defence of the information space.

A particularly significant fact is that this technological pressure has even forced the Russian military to make less secure decisions, such as the use of open, unencrypted radio frequencies for tactical communications, which allowed them to be intercepted. This fact highlights not only Russian operational weaknesses but also demonstrates the high level of technological competence achieved by Ukraine, even in an environment as complex and hostile as the cyber battlefield.

These developments have captured the attention of the international community, not only because of the impact of the conflict itself, but also because of the value they offer for strategic analysis and the formulation of new cooperation policies on security and defence in the digital sphere. A clear example is Ukraine's extraordinary collaboration with its Western allies and major technology companies such as Microsoft and Google, which have provided support in the areas of digital infrastructure, cybersecurity and cloud storage.

A key lesson that can be drawn from this practical experience, even though the conflict is not yet over, is therefore that, despite the complexity and multidimensional nature of cyberspace, there are real opportunities to establish effective defence mechanisms. There is no doubt that this defence is strengthened through civil-

military, public-private and international cooperation, taking shape as a new model of collective security in the cyber domain that can serve as a benchmark for future conflicts.

In other words, the main lesson is not that digital defence eliminates vulnerability, but that a resilient architecture can significantly reduce the impact of attacks and raise the strategic cost to the aggressor.

7 The challenge of modernising European defence strategy

Although the EU and NATO have strengthened their strategic framework against hybrid threats, with initiatives such as the aforementioned Strategic Compass or NATO's New Strategic Concept, the Ukrainian case highlights a persistent gap between the formulation of objectives and the actual availability of operational capabilities. The technical difficulty of attributing cyberattacks, the fragmentation of national capabilities, the diversity of doctrines and the absence of a fully integrated chain of command limit the speed and effectiveness of the European response.

The Russian invasion of Ukraine has marked a turning point for European security, as, for the first time since the end of the Second World War, the European continent is directly facing a high-intensity armed conflict on its doorstep, with profound implications for both regional stability and the international order.

This scenario has highlighted the structural vulnerabilities of the European defence system and has reignited the importance of NATO's strategy, whilst driving an accelerated rethinking of digital security and common defence policies within the EU.

This urgency to modernise capabilities in the face of a new type of multidimensional and technological warfare means that Europe faces a major strategic challenge involving a rethinking of its collective defence structure, as well as its digital autonomy and capacity to respond to conventional and non-conventional threats.

Indeed, Russian aggression has not only shattered the security architecture that Europe had built following the collapse of the Soviet Union in 1991 (Artola, 2023), but has also highlighted the return of a logic of competition between great powers.

In this new geopolitical landscape, both the EU and NATO have stepped up their security and defence policies, bolstering their deterrence capabilities in the face of increasingly complex threats, such as those of a hybrid nature; however, the existence of strategic instruments does not automatically equate to an integrated response capability, where three fundamental limitations persist:

1. Military fragmentation: The 27 Member States maintain divergent weapon systems, disparate national doctrines and differing geostrategic priorities, which leads to costly duplication and hinders interoperability (Segoviano, 2022).
2. Political inequality: Not all Member States perceive the same threats with equal intensity, and national interests frequently take precedence over collective action. In other words, for the EU to develop autonomous external action, Member

States must be in political agreement, enabling a robust and comprehensive strategy to tackle large-scale crises (De Castro and Borrajo, 2019).

3. Lack of integrated command: Despite institutional progress, Europe lacks a clear and effective command structure to manage military crises autonomously. The absence of a fully functional strategic decision-making process for all Member States limits the capacity for rapid reaction, thereby restricting the EU's potential as an independent military actor in the international system.

Consequently, these limitations explain why the European response has been stronger at the normative level than at the strictly operational level. These limitations hinder interoperability between national armed forces and, consequently, the EU's ability to project itself as an autonomous security actor in hostile scenarios. Thus, the challenge lies not only in designing new strategies, but in transforming them into effective, interoperable and sustainable capabilities. These challenges must be addressed urgently and in a coordinated manner so that Europe is capable of playing a significant role in this area within the new geopolitical order.

In other words, European security cannot be sustained solely through diplomatic stability; rather, an interoperable military capability is required that can adapt to a hostile environment characterised by strategic volatility and increasing unpredictability, as the main gap remains between normative ambition and effective operational capability.

To achieve this profound transformation, it is essential to heed the key lessons from the conflict involving the aggression against Ukraine, which cannot be ignored and must serve as inspiration for maintaining a credible and effective defence posture for Europe.

7.1 Lessons for Europe

The Ukrainian experience offers four main lessons for European defence. Firstly, doctrine must integrate cyberspace and disinformation as central domains of conflict. Secondly, technological capabilities must translate into real interoperability and not merely into modernisation programmes. Thirdly, public-private cooperation must cease to be the exception and become a structural component of defence. Fourthly, coordination between the EU and NATO must be geared towards faster, more integrated and sustainable responses to hybrid threats.

1. Multi-domain doctrine: Cyberspace and disinformation must be integrated as central operational domains, not as auxiliary areas. The cyberattacks against Ukrtelecom and Russian fake news campaigns demonstrate that these instruments can degrade critical infrastructure and erode social cohesion, with strategic effects equivalent to kinetic operations. Consequently, cyber defence ceases to be an auxiliary or complementary field, becoming instead a strategic priority in wartime situations. The ability to withstand, respond to

and recover from hybrid threats constitutes an essential component of national and European resilience.

2. Genuine technological interoperability: Technological capabilities, such as AI, UAVs, or real-time data analysis, must translate into systems that are interoperable between states and with NATO, rather than remaining isolated national programmes. The experience of Palantir, GIS ARTA and Delta in Ukraine demonstrates the multiplier effect of integrated platforms. In other words, the use of technology has altered the conventional tactical balance, necessitating an urgent review of defence and security culture; a clear example of this is the ease with which drones can be deployed, as well as their low cost (compared to other conventional systems), which poses an immediate challenge regarding the integration of these technologies across all European armed forces. Another example is the use of AI as an enabler of military strategy due to the ease of real-time data analysis for decision-making, as this represents a clear advance that constitutes supremacy on the battlefield and in the operations conducted there, whether at the physical or cyber level.

3. Structural public-private cooperation: Collaboration with technology companies (Microsoft, Google, Clearview AI) must move beyond *ad hoc* arrangements to become a permanent feature of European defence. Ukraine survives thanks to this hybrid civil-military-technological ecosystem. In other words, Ukraine's cooperation with private companies has harnessed the potential of emerging technologies to improve tactical warfare, providing greater assurance of the safety and integrity of troops, as well as optimising resources.

4. Accelerated EU-NATO coordination: European military mobility must be complemented by harmonised land, air and sea routes that enable rapid deployments. The current logistical fragmentation makes effective responses to high-intensity crises impossible.

In short, 21st-century security plans cannot be divorced from technological innovation; rather, they must adapt to it in order to provide an effective defence capable of minimising and mitigating the potential hybrid threats that a Member State or its allies may face, adapting in all cases to the new challenges posed by the Global Health Crisis.

It goes without saying that this strategic modernisation of common defence not only requires political will and technological advances, but must also overcome various structural obstacles that may limit its effectiveness.

In other words, this modernisation of European defence policy is not merely technological, but organisational and institutional. Europe must move from designing strategies to building effective, interoperable and sustainable capabilities. The EU has before it the opportunity to establish itself as an autonomous and resilient strategic actor in the global order. The strategic question is no longer whether it should modernise, as the answer is clear, but whether it will do so with the speed, scale and determination demanded by the new geopolitical environment.

8 Conclusions

The analysis carried out confirms that contemporary warfare has transcended the exclusively kinetic realm to become a multi-domain phenomenon in which new and potential threats capable of destabilising a country have emerged, such as cyberspace, disinformation and emerging technologies, which contain harmful elements that directly affect national and collective security and function as structural instruments of strategic coercion, not merely as operational supplements.

In response to the research question posed regarding the extent to which the war in Ukraine has altered the understanding and design of European defence against hybrid threats and cyberattacks, this study demonstrates that the Ukrainian conflict has acted as a catalyst for three fundamental transformations:

1. Conceptual: Hybrid warfare is no longer a theoretical concept, but a verifiable operational reality that combines conventional military operations with cyberattacks (e.g. Ukrtelecom), mass disinformation campaigns and disruptive technologies (AI, drones, predictive analytics). The conflict in Ukraine has clearly demonstrated that cyberspace is no longer merely a complementary arena in traditional warfare, but constitutes a central front in 21st-century armed conflicts. Far from being a domain reserved exclusively for the most resource-rich powers, the experience of Ukraine shows us how other states, with a solid, coordinated and comprehensive digital strategy—and in this case, with international support and cooperation with public and private actors—can combat attacks in cyberspace and build a resilient and effective digital defence. For the use of cyberspace does not entail solely attacks on a country's critical infrastructure, but also encompasses other operations such as disinformation or digital sabotage, which determines the need for a comprehensive, agile and multidisciplinary response. Ukraine demonstrates that technological superiority depends less on the volume of resources than on the capacity for real-time integration and adaptation.
2. Doctrinal: Cyberspace has established itself as a central operational domain, where institutional resilience is as decisive as offensive capabilities. Ukrainian digital defence, supported by public-private cooperation (such as with Palantir, Microsoft and Google), demonstrates that medium-sized states can counter superior cyber powers through hybrid civil-military architectures.
3. Institutional: Europe faces a persistent gap between strategic ambition (Strategic Compass, NATO's New Concept) and actual operational capability, constrained by military fragmentation, political divergences and the absence of integrated command. The Ukrainian experience reveals that EU-NATO cooperation must be accelerated towards effective, interoperable and sustainable responses.

In this context, the fight against hybrid threats cannot be conducted in isolation, but requires a comprehensive cooperation strategy structured across various levels, yet in all cases based on rigorous knowledge and the coordination of national and

international experts. Indeed, this evidence imposes four unavoidable strategic imperatives on Europe:

- Multi-domain doctrine: Integrating cyberspace and disinformation as central domains of planning and operations.
- Real interoperability: Converting technological programmes into shared and effectively deployable capabilities.
- Hybrid ecosystem: Structuring civil-military, public-private and international cooperation and collaboration as essential pillars.
- Enhanced coordination: Harmonising EU-NATO efforts for rapid responses to high-intensity crises.

In light of the above, we can state that Russia's war of aggression against Ukraine has not only unleashed a devastating humanitarian crisis, but has also acted as a catalyst for profound transformations regarding the conceptualisation and nature of armed conflict today. Indeed, it is clear that this conflict has accelerated the transition from traditional warfare towards the model of hybrid warfare we are experiencing in the 21st century, in which conventional military operations are combined with tools and methods from cyberspace, disinformation and the use of emerging technologies such as AI or drones.

In this context, we can conclude that technology has not only established itself as an enabler of military capabilities, but has also become a structural component of security and defence strategy itself. It is clear that Ukraine's experience offers valuable lessons today, even though the conflict is not yet over, as it highlights the need to adapt digital capabilities, invest in resilience, and foster technological cooperation in high-intensity scenarios such as armed conflict. This conflict highlights the urgent need for Europe and its allies to strengthen their digital and technological policies with the aim of enhancing their defensive capabilities and response mechanisms to hybrid threats.

The reshaping of the European geopolitical balance resulting from this conflict also highlights the fact that security cannot be understood solely in military terms, but requires a broader perspective that also incorporates technological innovation and cyber defence, as well as the strengthening of strategic alliances and greater integration between state and non-state actors. All in all, analysis of this conflict to date suggests that the future of warfare has already begun and that preparation, cooperation and technological adaptation are required to face the challenges of the new international order with greater confidence.

In short, the Ukrainian case not only illustrates the new 21st-century paradigm of warfare but also poses a concrete challenge: to modernise European defence not through declarations of intent, but through real, interoperable and deployable capabilities that enable hybrid threats to be countered with the speed and effectiveness demanded by the new geopolitical environment.

The main contribution of this article is not merely to describe the transformation of warfare, but to demonstrate that this transformation requires Europe to undertake a profound review of its doctrinal, industrial and organisational frameworks. The

decisive question is no longer whether technology changes warfare, but what kind of political and strategic architecture enables this transformation to be turned into a real defensive advantage.

Bibliography

Alastuey Rivas, J. *et al.*. (2024). *La desinformación como arma de guerra* [online]. IEEE Opinion Paper 26/2024. [Accessed: 2026]. Available at: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinformacion.pdf

Artola Kortam, M. (2023). Rusia y Ucrania: Una mirada desde la historiografía reciente [online]. *Cuadernos de Historia Contemporánea*. 45, pp. 423–430. [Accessed: 2026]. Available at: https://doi.org/10.5209/chco.87941

Aydemir, E. (2022). *Ukraine's cognitive warfare operations against Russia: representation, story and micro-mythology*. Avrasya Uluslararası Araştırmalar Dergisi. 10(32), pp. 358-367.

Baqués, J. (2017). *Hacia una definición del concepto de «Gray Zone» (GZ).* Research Paper by Instituto Español de Estudios Estratégicos (IEEE).

Colom Piella, G. (2020). Anatomía de la desinformación rusa. *Historia y Comunicación Social*. 25(2), pp. 473–480.

—. (2022). Las estrategias de la OTAN en respuesta a los conflictos híbridos [en línea]. *CIDOB.* [Accessed: 2026]. Available at:https://www.cidob.org/publicaciones/las-estrategias-de-la-otan-en-respuesta-los-conflictos-hibridos

Council of the European Union. (2024). Una Brújula Estratégica para la Seguridad y la Defensa [online]. *consilium.europa.eu.* [Accessed: 2026]. Available at:. https://www.consilium.europa.eu/es/policies/strategic-compass/

—. (2025). Cómo refuerza la UE su ciberseguridad. [online]. *consilium.europa.eu.* [Accessed: 2026]. Available at: https://www.consilium.europa.eu/es/policies/cybersecurity/

De Castro, J. L. and Borrajo, D. (2019). El futuro de la seguridad y la defensa en la UE post-Brexit: el salto a la integración. *Cuadernos Europeos De Deusto.* 60, pp. 187–217. [Accessed: 2026]. Available at: https://doi.org/10.18543/ced-60-2019pp187-217

European Union. (2025). European Parliament resolution of 2 April 2025 on the implementation of the common foreign and security policy – annual report 2024 (2024/2080(INI)). *Official Journal of the European Union.*

Fiott, D. (2022). The Fog of War: Russia's War on Ukraine, European Defence Spending and Military Capabilities [online]. *Intereconomics*. 57, pp. 152–156. [Accessed: 2026]. Available at: https://doi.org/10.1007/s10272-022-1051-8

Franco, J.D. (2023). Guerra híbrida: críticas y retos del conflicto moderno. *Revista Estado, Paz y Sistema internacional.,* 2(4), pp. 19–204.

Franke, U. and Söderström, J. (29 September 2023). *Star 'Tech' Enterprise: Tecnologías emergentes en la guerra rusa contra Ucrania* [online] [Accessed: 2026]. Available at:. European Council on Foreign Relations. https://ecfr.eu/madrid/publication/star-tech-enterprise-tecnologias-emergentes-en-la-guerra-rusa-contra-ucrania/

Gutiérrez de León, B. (2021). Amenazas híbridas y zona gris. OTAN, Unión Europea y España ante esta nueva forma de enfrentamiento [online]. *Global Strategy Reports*. [Accessed: 2026]. Available at: https://global-strategy.org/amenazas-hibridas-y-zona-gris-otan-union-europea-y-espana-ante-esta-nueva-forma-de-enfrentamiento/

MCDC. (2017). *Understanding Hybrid Warfare* [online]. MCDC. [Accessed: 2026]. Available at: https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

Ministerio de Defensa. (2022). *Nuevo Concepto Estratégico de la OTAN* [online]. Ministerio de Defensa. [Accessed: 2026]. Available at: https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

NATO. (2016). *Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw* [online]. Nato.inc. [Accessed: 2026]. Available at:. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Rodríguez, E. *et al.* (2023). *La inteligencia artificial en la guerra híbrida como arma de desinformación* [online] Documento de Opinión IEEE 61/2023. [Accessed: 2026]. Available at: https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO61_2023_EDUROD_Inteligencia.pdf

Segoviano Monterrubio, S. (2022). Conflict scenario analysis. In: López Garrido, D. (ed.). *La defensa europea y la Europa de la defensa. Informe 2022.* pp. 23–42. Fundación Alternativas.

Silva Ramirez, F. (2022). Operaciones en la "Zona Gris": ¿de qué estamos hablando ?. *Escenarios Actuales año. 27*, pp. 107–121. Centre for Military Studies and Research, Army of Santiago de Chile.

State Service of Special Communications and Information Protection of Ukraine - SSSCIPU. (2022). *Cyberattack against Ukrtelecom on 28 March: the details* [online]. [Accessed: 2026]. Available at: https://cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali

Article received: 11 February 2026
Article accepted: 28 April 2026