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

Antonio Legaz
Cyber Defense Analyst

Mail: alegazs@indra.es

The end of surprise? A study on the mutation of the element of surprise in the century of (dis)information

Abstract

The revolution in information gathering and analysis has transformed the role of surprise in modern warfare. Surveillance technologies, Big Data analytics and artificial intelligence have drastically reduced strategic uncertainty, limiting the ability of actors to execute surprise attacks. However, this apparent end of surprise faces a growing challenge: disinformation. The proliferation of false information, data manipulation, and information poisoning have generated a new type of "digital fog of war," in which information overload and strategic noise can generate false certainties. This paper explores how surprise has been transformed in the information age and how the struggle between transparency and deception continues to define the modern battlefield. Finally, it discusses the role of intelligence analysis in converting data into useful knowledge, highlighting the importance of distinguishing between truthful information and strategic manipulation to avoid critical vulnerabilities.

Keywords

Surprise, misinformation, uncertainty, cognitive biases.

Cite this article:

Legaz, Antonio (2025). "The end of surprise? A study on the mutation of the element of surprise in the century of (dis)information". Journal of the Spanish Institute for Strategic Sudies, No.25, pp. 337-356.

1 The element of surprise and its historical importance

1.1 to surprise

What do the Japanese attack on Pearl Harbor in 1941, the German invasion of the Soviet Union in 1941 (Operation Barbarossa), the invasion of Norway in 1940 and the Egyptian and Syrian attack on Israel in 1973 (Yom Kippur War) have in common? All these key operations of the 20th century were made possible by one determining factor: surprise.

In the intricate tapestry of military strategy, surprise has been an essential principle in military strategy, a resource that can drastically alter the balance of power in a conflict. Surprise not only affects tactics and strategy, but also influences the psychology of the adversary, generating disorientation and chaos (Betts, 1982: 87-105). Its effectiveness lies in the ability to disarticulate the enemy's plans, sow uncertainty and exploit the tactical advantage with a force that, in other circumstances, might otherwise seem insufficient. It is not only a matter of attacking without warning, but of manipulating the adversary's perception in order to reduce his capacity to respond.

Surprise, in its purest essence, seeks to generate an asymmetry in the opponent's position, disarticulating his plans and sowing confusion and discouragement in his ranks. This destabilizing effect not only translates into a tactical advantage, but also amplifies the impact of military actions, allowing a smaller force to overcome a larger one. For this reason, surprise has been considered the ideal means of achieving relative numerical superiority at the decision point, even in the absence of absolute superiority.

Throughout history, commanders and strategists have resorted to surprise to compensate for numerical or technological inferiorities. Surprise is not limited to mere concealment of intentions, but can also be achieved through speed, flexibility and boldness in execution (Handel, 1984: 220-281). Frederick the Great, for example, based his 1760 campaign on unexpected maneuvers that destabilized the Austrian army, demonstrating that surprise is not only an act of stealth, but also of strategic innovation.

The achievement of surprise, far from being a fortuitous act, requires a conjunction of factors that include secrecy in preparation, celerity in execution and the determination of both the government and the commanding general (Clausewitz, 1832: 198-204). However, despite its importance, success in the realization of surprise is never guaranteed, and on multiple occasions, the friction inherent in warfare hinders its materialization. Despite the challenges it poses, the principle of surprise remains a fundamental pillar of strategy, influencing decision making and the conduct of military operations throughout history.

It is essential to note that surprise is not limited to offensive actions but is also a valuable resource in defense. The ability to anticipate enemy movements and prepare defenses unexpectedly can confer a significant advantage. For example, the

Spanish resistance against Napoleon demonstrated that surprise could also arise from mobilization and determination, which through guerrilla warfare, unforeseen attacks and tenacious resistance managed to destabilize the invading army.

1.2 Taxonomy of surprise

The systematic study of strategic surprise requires transcending the traditional dichotomy between success and failure by means of a functional categorization that allows a structured analysis of the phenomenon. Following a taxonomic approach, it is possible to identify four main modalities: "capability surprises", manifested when the adversary deploys unknown technologies or methods, as evidenced by the Soviet Typhoon class submarines, whose stealthy properties severely compromised Western detection systems (Paredes and Oliveira, 2023:4-6). The "surprises of intent", paradigmatically exemplified by the attack on Pearl Harbor, where despite knowledge of Japanese capabilities, their strategic objectives were misinterpreted. The "surprises of execution", illustrated by Operation Barbarossa, where the surprise factor was not in the what but in the how of the tactical implementation. Finally, the "temporality surprises", characterized by the unexpected materialization of anticipated threats, as occurred with the Tet Offensive during the Vietnam War.

This taxonomy, far from being a mere academic exercise, enables the development of specific preventive strategies of differentiated anticipation (Zwitter, 2015: 9-11). Thus, to counter capability surprises, sustained investment in technological intelligence and counterintelligence is imperative. In the face of intent surprises, a rigorous psychological and contextual analysis is required, implementing hostile actor profiling techniques such as those proposed by Borum[1] (2004: 22-25). In the case of execution surprises, simulation and modeling of unconventional scenarios are essential. Finally, temporality surprises require early warning systems based on the detection and interpretation of weak indicators and signals.

The historical evolution of strategic surprise, from the classic Trojan horse to contemporary hybrid threats, reveals recognizable patterns through the lens of this categorization, allowing parallels to be drawn and lessons to be learned that are applicable to today's environment. However, the changing nature of conflict demands a continuous review and updating of this taxonomy, avoiding the risk of preparing exclusively for already experienced modes of surprise. Recognition of these categories not only facilitates retrospective analysis but, crucially, guides the development of adaptive defensive capabilities in the face of a phenomenon that, despite its longevity,

1 Borum proposes a multifactorial analysis framework for understanding the motivations of hostile actors that integrates four dimensions: the evaluation of the ideological-doctrinal context, the analysis of radicalization processes, the study of situational precipitating factors and the identification of predictive behavioral indicators. Its "Four-Stage Pathway to Terrorism" methodology allows the sequential decomposition of the decisional process leading to hostile action.

continues to represent one of the most formidable challenges to contemporary strategic security.

This multidimensional approach to strategic surprise is a significant advance over traditional explanatory models, which are overly focused on intelligence failures or individual cognitive biases. The proposed taxonomy integrates technological, psychological, operational and temporal factors, offering a comprehensive analytical framework that transcends the limitations of previous monolithic approaches.

1.3 Surprise in the 21st century

From Clausewitz (1832) to Van Creveld (1991), war has been described as a phenomenon dominated by uncertainty. The concept of the "fog of war", a term coined by Clausewitz, alludes to the difficulty of obtaining clear and precise information on the battlefield. Throughout history, this fog has been an ally of surprise: chaos, misinformation and friction have allowed strategists to exploit gaps in enemy perception. In the 21st century, however, the proliferation of surveillance technologies appears to be dissipating that fog, reducing the scope for surprise.

The revolution in military intelligence has been marked by the development of technologies such as observation satellites, massive data analysis and artificial intelligence applied to pattern detection (Allen and Chan, 2017: 45-62). In the Cold War, the launch of CORONA, the first U.S. surveillance satellite program, already made it possible to accurately monitor Soviet military activity, hindering the possibility of large-scale surprise attacks (Perry and Carter, 1999: 114-120). Today, the surveillance capability is exponentially greater: by 2022, more than 10,000 satellites were orbiting the Earth, many of them equipped with high-resolution sensors, SAR (Synthetic Aperture Radar) technology and artificial intelligence for real-time analysis of geospatial imagery (Weeden and Samson, 2022: 32-47).

This unprecedented access to detailed information directly affects the dynamics of modern conflict. For example, during the war in Ukraine, Western intelligence detected months in advance Russian preparations for the 2022 invasion. Intelligence reports based on satellite imagery and telecommunications traffic data made it possible to anticipate Russian military movements, leading Ukraine and its allies to better prepare for the offensive (Freedman, 2022: 178-196).

Added to this satellite surveillance is the impact of Big Data in predicting war scenarios. Machine learning algorithms analyze patterns in social networks, economic transactions and logistical movements to foresee military actions before they occur (Taddeo and Floridi, 2018: 723-735). This type of predictive intelligence was used, for example, in the fight against the Islamic State in Syria and Iraq, where U.S. drone strikes were guided by data analytics that revealed patterns of fighter behavior (Schmidt, 2020: 56-73).

The key question is: is surprise still possible in the age of total surveillance and massive data analysis? History shows us that, even as intelligence tools evolve, surprise

remains a compelling factor. The question, therefore, is not whether surprise has disappeared, but how it has been transformed to adapt to a new battlefield.

1.4 Objectives

This paper aims to analyze, from a multidisciplinary perspective that integrates security studies, strategic communication and cognitive psychology, the transformation of the element of surprise as a decisive factor in contemporary confrontations. To this end, five fundamental questions are posed, the answers to which will allow us to understand the evolution, current state and future projection of this phenomenon:

1. How has the element of surprise in modern conflicts mutated in the face of the proliferation of surveillance and mass data collection technologies?
2. To what extent have technological tools such as satellites, Big Data and psychological profiling changed the ability of state actors to execute or prevent surprise attacks?
3. What role does disinformation play as a counterweight to information transparency and as a new vector for generating strategic surprise?
4. Why do anticipation failures continue to occur despite advanced surveillance and information analysis systems?
5. What is the future of the element of surprise in a world where the abundance of information can paradoxically increase strategic uncertainty?

These questions, approached from both a historical and contemporary perspective, form the analytical framework through which this paper aims to offer a vision of how the element of surprise has evolved without disappearing, adapting and transforming itself to remain a decisive factor in the conflicts of the 21st century.

2 Massive data collection tools

2.1 Satellites: an end to the fog of war

The 21st century has witnessed an explosion in the military use of space. Observation satellites have transformed the way states access strategic information, significantly eroding the capacity for surprise in warfare (Weeden and Samson, 2022: 18-40).

In 2022, more than 2,000 satellite launches were recorded, and in 2023 the total number of objects in orbit exceeded 10,900 (Union of Concerned Scientists, 2023: 3-7). This growth is not merely technological but reflects the increasing militarization of space. Satellites that were once limited to weather observation and communications tasks now play a key role in military intelligence, surveillance and reconnaissance (ISR).

The effectiveness of these systems is evident in recent conflicts. During the Russian invasion of Ukraine in 2022, satellite imagery from Maxar Technologies and

intelligence analysis from Starlink X enabled Ukraine to detect and anticipate Russian troop movements (Freedman, 2022: 215-233). For the first time in history, access to satellite imagery was not restricted to major powers, but became a tool available to smaller governments and even private actors and NGOs.

The importance of satellites in dispelling the fog of war lies in their ability to obtain detailed and accurate information, which is achieved through different observation technologies.

The satellites use active remote sensing, based on synthetic aperture radars (SAR) that emit radio waves and analyze the time they take to return. This technology makes it possible to detect objects and measure distances with high precision, even in adverse conditions such as clouds or darkness. SAR systems are capable of measuring the time of flight of the pulse from the time it leaves the satellite until it reaches the Earth and returns, allowing to know how far away an element is, in addition, they analyze the degree of absorption and penetration of the wave on the surface, which allows to obtain information not only geometrically, but also on the composition of the surface.

Passive remote sensing captures sunlight reflected by the Earth, similar to a camera. This technology provides high spatial resolution images, but their quality is affected by cloud cover and time of day. Passive remote sensing satellites, such as Sentinel-2, offer a spatial resolution of 10 meters. Military satellites also use infrared sensors that enable heat detection, which is useful for identifying activities in the dark, as well as tracking changes in the temperature of certain areas and groups of people. During the war in Syria, these sensors were used to identify the transport of chemical weapons in areas controlled by the Assad regime (Futter, 2018: 135-140). In addition, they employ multispectral and hyperspectral loading, capable of detecting light in multiple bands of the electromagnetic spectrum. This has been key in detecting clandestine nuclear facilities, as was the case with the Iranian program at Natanz (Kemp, 2014: 39-78).

A recent trend is the use of nanosatellite swarms. Unlike traditional satellites, these low-cost devices can work in a network, providing real-time imagery and reducing the risk of a single unit being destroyed or disabled (Pelton, 2020: 1-20). For example, the PlanetScope program operates with hundreds of small satellites in low orbit, allowing continuous monitoring of the planet with daily updates.

In Spain we have the Spanish satellite PAZ that materializes some of these technological advances. This is an active remote sensing platform that sends 33 images daily, with the ability to detect surface changes of up to 2-3 mm by means of interferometry, which makes it possible to identify areas where land has been disturbed or where mines have been buried, monitor the position and course of 170,000-200,000 vessels at all times thanks to its AIS (Automatic Identification System) technology, track moving targets, such as military vehicles and convoys according to data from the International Maritime Organization.[2]

2 International Maritime Organization (2022) 'Annual Shipping Report 2022', London: IMO: 85-93.

The current level of surveillance poses challenges to any military seeking to conduct a surprise operation. The accumulation of real-time data, combined with artificial intelligence algorithms, makes it possible to identify patterns and anticipate moves before they are executed. A prime example is the Pentagon's Project Maven system, established as a multifunctional algorithmic warfare team, which uses AI to analyze tactical surveillance imagery and detect up to 38 classes of critical objects, including attack preparations or insurgent movements in conflict zones (Work, 2017: 1-2; Pellerin, 2017: 2-3). The system employs biologically inspired neural networks and deep learning techniques to automatically process drone images and videos, accurately identifying military vehicles, weaponry, fortifications, and troop movements without direct human intervention. This allows a single analyst to process up to three times more information than before, working symbiotically with algorithms to transform the massive volume of surveillance data into actionable intelligence (Pellerin, 2017: 3-4).

Satellite technology is not only capable of detecting physical activity, but also operations in the electromagnetic spectrum. Satellites equipped with synthetic aperture radar (SAR) such as Sentinel-1 have demonstrated the ability to detect electronic jamming directed against GPS systems. In a study documented by the European Space Agency (2020: 34-42), jamming patterns detected over conflict zones in Syria and eastern Ukraine were analyzed, where SAR systems picked up anomalies consistent with electronic warfare activities. These electromagnetic signatures make it possible to identify positions from which jamming operations are being conducted, even when physical equipment is concealed or camouflaged. These capabilities represent a significant change in the transparency of the electromagnetic battlefield, traditionally invisible to direct observation (Papathanasiou, 2019: 125-137). This type of surveillance drastically reduces the possibility of tactical surprise in the cyber and electromagnetic domain, providing early warnings of hostile activities before they can materialize into conventional attacks.

2.2 Mind and digital: Big Data and profiling

If satellite surveillance has reduced the margin for physical surprise, the development of advanced psychological profiling tools combined with Big Data analysis has taken military pre-emption to a new level. Through the massive analysis of data, behavioral patterns and psychological predictions, states can foresee strategic decisions of their adversaries with unprecedented accuracy (Taddeo and Floridi, 2018: 723-735).

The concept of psychological profiling applied to warfare is not new. Sun Tzu already warned that knowing the enemy was as important as knowing one's own army. However, in the 21st century, this idea has materialized in artificial intelligence systems that analyze the behavior of political leaders, military and hostile organizations to predict their actions (Kahneman and Renshon, 2007: 34-48).

A clear example of this trend was the intelligence operation prior to the invasion of Iraq in 2003. U.S. intelligence agencies used personality analysis to assess Saddam

Hussein's likely responses to various military and diplomatic pressures (Post, 2003: 175-190). Today, tools such as computational leadership profiling make it possible to predict with a high degree of certainty the likelihood that a leader will opt for war, diplomatic engagement, or nuclear deterrence (Renshon, 2021: 53-71).

Modern psychological profiling is based on the analysis of several variables to predict behavior and reduce surprise in strategic decisions. One of the key aspects is the study of an individual's personal history and ideological beliefs. A recent example is the analysis of Vladimir Putin's behavior, whose past as a KGB agent and his view of Russian nationalism have been instrumental in anticipating his strategic moves (Hill and Gaddy, 2015: 98-112). In addition, decision-making patterns are another important factor, as recurrent cognitive biases have been identified in political and military leaders. For example, the overconfidence bias was observed in both Hitler in 1941 and Israel before the Yom Kippur War in 1973, and has been incorporated in models to predict strategic decisions (Levy, 1994: 279-312).

In the construction of psychological profiling, the analysis of language and non-verbal behavior also plays a crucial role. Artificial intelligence algorithms have been trained to detect signs of aggression or conciliation in public speeches. Intelligence agencies regularly employ behavioral analysis techniques to evaluate foreign leaders (Fingar, 2011: 112-129).

On the other hand, Big Data has revolutionized military intelligence by enabling the analysis of massive amounts of information in real time. Whereas in the past military analysts relied on fragmented reports and human sources, today algorithms can detect hidden patterns in data ranging from banking transactions to social network interactions (Allen and Chan, 2017: 63-85).

One example of its impact is the fight against terrorism. Advanced data analytics systems developed by security agencies can monitor digital communications and detect patterns of radicalization. Case studies show that these systems can identify specific indicators of radicalization in online environments, such as changes in language patterns, consumption of extremist material and increased participation in radical forums (Behr *et al.*, 2013: 42-47). This digital surveillance is complemented by social network analysis methods that allow the identification of recruitment patterns used by organizations such as the Islamic State, facilitating the neutralization of terrorist cells before they execute attacks (Berger and Morgan, 2015: 4-20).

In the realm of conventional warfare, predictive analytics based on Big Data has been key in recent conflicts. During the war in Ukraine, Western intelligence used predictive models based on analyses of economic, logistical, and military movement data to anticipate the Russian invasion weeks before it occurred (Freedman, 2022: 250-267).

Despite their advantages, these tools are not infallible. Information overload and the proliferation of false data can generate analytical paralysis, a phenomenon in which decision makers are overwhelmed by an excess of data without being able to draw clear conclusions (Tetlock and Gardner, 2015: 25-40).

In addition, strategic deception remains a key factor in warfare. Actors such as Russia and China have perfected the use of disinformation to manipulate the perception of their adversaries. During the annexation of Crimea in 2014, Russia used a combination of disinformation and covert operations to conceal its intentions until the occupation was a fait accompli (Galeotti, 2017: 85-103).

Technological advances have reduced the margin for uncertainty, but surprise has not disappeared. Information, however abundant it may be, is only useful if it is analyzed accurately and without falling into false certainties. History has shown that it is not the lack of data that generates vulnerability, but the way it is interpreted and integrated into decision making (Fingar, 2011: 112-129).

3 Disinformation: the great obstacle in the Information Age

3.1 From analog to digital disinformation

Although massive access to information and new technologies have enabled unprecedented data collection, these advances do not guarantee better decision making if the information collected is erroneous or manipulated. Predictive intelligence and strategic analysis depend not only on the amount of data available, but also on its veracity and the ability to correctly interpret the patterns that emerge from it. However, in an information-saturated environment, where misinformation and information manipulation have become key strategic tools, differentiating between reliable data and intentional deception is an increasing challenge.

The manipulation of information for strategic purposes is a practice as old as war itself. Since time immemorial, armies and governments have used disinformation to confuse the enemy, weaken his morale or influence the perception of the population. Sun Tzu already warned that all warfare is based on deception, highlighting the importance of making the adversary believe that one is weak when one is strong, or that one will attack from one flank when one will attack from another. Throughout history, deception has played a crucial role in numerous conflicts, demonstrating that the perception of reality can be as decisive as reality itself.

A classic example of this is Operation Fortitude during World War II, in which the Allies carried out an elaborate hoax to make the Nazis believe that the landing in France would occur in Pas-de-Calais instead of Normandy (Holt, 1978: 53-68). Fake troop movements, deceptive radio transmissions, and even the creation of a dummy army with inflatables and decorations were used to reinforce the illusion of an imminent invasion at the wrong point. This deception was so effective that even after June 6, 1944, when Allied troops had already landed in Normandy, the Nazis continued to believe that it was a diversion and that the real offensive would be at Pas-de-Calais, delaying their response.

Today, disinformation has become a global phenomenon, enhanced by the massive access to social networks and the growth of digital platforms that allow

the instantaneous dissemination of content without rigorous verification. The annexation of Crimea in 2014 is a clear example of the contemporary use of these strategies. Russia employed a combination of covert military action and an intense disinformation campaign to justify the intervention to domestic and external public opinion (Galeotti, 2017: 42-58). False narratives were created depicting Russian forces as local "self-defense groups," while state media propagated the idea that the Ukrainian government was controlled by extremists, hindering Western response and generating uncertainty.

In the 21st century, the proliferation of digital information has changed the rules of the game. False information is no longer spread exclusively through pamphlets or radio but goes viral in a matter of minutes via social networks. During the 2016 US presidential election, research revealed that thousands of automated accounts, many linked to Russia, were involved in the dissemination of misleading information with the aim of polarizing public opinion and eroding trust in democratic institutions (Benkler *et al.*, 2018: 225-260). Through bots, conspiracy theories and fake news designed to influence the electorate were promoted, exacerbating pre-existing divisions in American society.

From a strategic point of view, disinformation is no longer simply a propaganda tool; it has become a political and military weapon with the potential to destabilize governments and manipulate perceptions of reality. The speed with which these false narratives spread, combined with the difficulty of effectively disproving them, makes disinformation operations more dangerous than ever. Unlike traditional wars, where armies clash on the battlefield, the information war is fought in the minds of the population, where truth and lies compete for dominance.

History has shown that control of information is as important as control of territory. In a world where information flows without restriction, the ability to distinguish between truth and manipulation is an increasingly complex challenge for governments and citizens alike.

3.2 New disinformation methods

The impact of misinformation on intelligence analysis is particularly serious, as it undermines the credibility of sources and makes it difficult to make decisions based on verifiable facts. Analysts must already contend with their own cognitive biases in interpreting data, but when information is deliberately manipulated, the risk of erroneous conclusions increases exponentially (Heuer, 1999: 111-126). This situation is driven by the proliferation of technological tools designed to amplify information manipulation.

Bots and trolls operate as digital armies designed to flood the information space with specific narratives, making it difficult to identify legitimate sources and generating confusion in public opinion. In recent conflicts, such as the war in Ukraine, these methods have been used to fabricate a distorted perception of the

confrontation, destabilizing society and reducing the ability of intelligence analysts to get a clear picture of the unfolding events. Also, deepfakes, for their part, represent a breakthrough in audiovisual manipulation, allowing the creation of fake videos that can attribute statements or actions to political and military actors without them having carried them out. This technology has enormous disruptive potential in the military field, where trust in the authenticity of information is key. The possibility of disseminating falsified videos with speeches by military or political leaders can generate chaos, confusion and erroneous decisions based on manipulated information.

At the same time, the falsification of documents continues to be one of the most widely used strategies in military disinformation. Leaked and modified documents can influence diplomatic negotiations, demoralize troops or provoke crises among allies. The manipulation of intelligence records, strategic reports and military orders has been used throughout history to induce errors in the operational planning of adversaries.

An aggravating factor in the problem of disinformation is the speed with which it spreads. In previous decades, information manipulation operations required months or even years to take effect, whereas today, with the presence of social networks and digital platforms, a fake news story can reach millions of people in a matter of hours. This phenomenon was reflected in the disinformation crisis during the COVID-19 pandemic, where conspiracy theories and manipulated data went viral, generating distrust in science and public health measures (Lewandowsky *et al.*, 2021: 80-127). The lack of effective regulation on the propagation of false content has allowed certain actors to exploit this situation for political or economic ends, eroding trust in institutions and polarizing entire societies.

Combating disinformation requires a multidimensional approach combining technology, education and regulation. The implementation of pattern detection algorithms is a promising strategy to identify disinformation networks in real time (Ferrara *et al.*, 2016: 96-104). However, there is also a risk that these algorithms may be biased and end up censoring valid information. Therefore, it is crucial that the development of these technologies is complemented by human oversight and transparency in their application mechanisms.

Another essential element in the fight against misinformation is media education. Studies have shown that critical thinking and the ability to evaluate information sources can significantly reduce the spread of fake news (McGrew *et al.*, 2018: 165-193). In this sense, some countries have implemented educational programs focused on teaching citizens how to identify manipulated content and how to verify the credibility of a source before sharing it. While these programs are a step in the right direction, their large-scale impact has yet to be demonstrated.

At the governmental level, international bodies such as the European Union have developed joint strategies to track and remove fake content from digital platforms (European Commission, 2020: 8-15). However, this type of measures raises a dilemma about freedom of expression, as the regulation of content on the Internet could be used by certain governments to censor legitimate criticism or silence dissent. The

solution lies in finding a balance between the protection of truthful information and respect for fundamental rights.

In the military and security domain, intelligence agencies have begun to adopt "intensive cross-checking" strategies to ensure the reliability of information before incorporating it into their analysis (Rid, 2020: 412-435). This involves contrasting sources of different provenance, analyzing patterns of disinformation, and tracing the origin of particular false narratives. However, the challenge remains monumental due to the overwhelming amount of information circulating daily in digital environments.

Combating misinformation also depends to a large extent on the responsibility of the traditional media. While the proliferation of social networks has decentralized the production and distribution of news, the media continue to play a crucial role in fact-checking and educating the public about the importance of cross-checking information. However, has also been responsible at times for spreading misinformation in their eagerness to be the first to report a story. This highlights the importance of journalistic ethics and the need for self-control mechanisms in information practices.

Thus, the phenomenon of disinformation not only affects the perception of reality, but also represents a tangible threat to global security, intelligence analysis and the stability of democracies. Tackling it requires a joint commitment between governments, technology companies, media and citizens to build a more resilient and critical society in the face of information manipulation.

4 The importance of analysis

We return to the initial question, beyond the surprise in their execution, what do the Japanese attack on Pearl Harbor in 1941, the German invasion of the Soviet Union also in 1941 (Operation Barbarossa), the German invasion of Norway in 1940 and the Egyptian and Syrian attack on Israel in 1973 (Yom Kippur War) have in common?

In all these cases, the victims made erroneous assumptions about the attacker's intentions and capabilities (Betts, 1982: 32-54). For example, the United States underestimated Japan's ability to carry out an attack on Pearl Harbor, while the Soviet Union did not believe that Germany would attack, despite signs of mobilization. In the case of the Yom Kippur War, Israel did not consider the possibility of a joint attack by Egypt and Syria, despite signs that they were preparing. Germany's invasion of Norway came as a surprise because Norway did not consider itself a priority target and believed in its neutrality.

Despite the fact that in all these cases there were signs that an attack was imminent, these signals were either not interpreted correctly or were ignored. The study of military surprise has shown that cognitive biases play a crucial role in these failures. Leaders tend to cling to their prior perceptions even when the evidence suggests the opposite, a phenomenon that is accentuated in environments of high uncertainty (Jervis, 1976: 58-84). In the case of Pearl Harbor, there was intelligence information indicating the possibility of an attack, but it was not given the necessary importance

(Wohlstetter, 1962: 382-401). Similarly, Stalin received warnings of the impending German invasion but chose to ignore them in the belief that Hitler would not open a second front in 1941 (Gorodetsky, 1999: 238-265). Similarly, in the Yom Kippur War, Israel did not consider the possibility of a full-scale Egyptian and Syrian attack, despite multiple warnings. The belief that Egypt would not risk war without air superiority led to ignoring troop movements on the border (Bar-Joseph, 2013: 145-162).

In most cases there were deception operations by the attackers to conceal their true intentions. Germany carried out disinformation operations to conceal its plans to attack the Soviet Union, and also in the case of Norway. Japan took steps to make it appear that it was negotiating with the United States when it was really preparing for attack.

These examples illustrate how a combination of erroneous assumptions, inattention to warnings, and inadequate preparedness make surprise attacks a phenomenon that palliates, not with better information, but with constant alertness and proper attention to elicitation analysis.

A failure to prevent surprise attacks often lies in an organization's inability to manage information properly, failing to distinguish between important signals and noise (Barnea and Meshulach, 2021: 43-59). Data overload can be as dangerous as data scarcity, as it can lead to analytical paralysis or incorrect prioritization of threats (Fingar, 2011: 75-91). During the invasion of Norway, Allied authorities received reports of unusual movements in the Kriegsmarine, but these were interpreted as routine maneuvers (Gannon, 2021: 35-48). A recurring problem in military intelligence is that warning signals are often ambiguous and require not only objective information, but also strategic intuition to be correctly interpreted (Heuer and Pherson, 2010: 132-148).

Effective analysis depends not only on the information available, but also on the organizational structure and the ability to challenge assumptions. As Handel (1984) mentions, intelligence must not only identify threats but also challenge pre-existing narratives within strategic decision making. This implies fostering critical thinking within intelligence agencies and avoiding the tendency to analytical conformism. A clear example of this problem was the over-reliance on nuclear deterrence during the Cold War, which led to dismissing the possibility of large-scale conventional conflicts (Luttwak, 1987: 189-205).

Thus, the primary mission of intelligence analysis is to provide timely information and insights that help decision-makers understand events with far-reaching implications for national interests (Fingar, 2011: 117-132). It is not just about presenting "facts," but about providing insights into trends, the political logic of foreign leaders, or how issues are perceived outside the country. In other words, analysis is what transforms raw data into useful intelligence.

The importance of the analysis is manifested in the assessment of enemy capabilities and intentions. The wartime capabilities of weapon systems cannot be automatically deduced from their technical characteristics, but depend on the operational concepts, strategy and tactics that would direct their use (Kam, 2004: 163-178). This implies that analysis is not limited to the collection of technical information but also requires an understanding of the context in which such technology is employed.

Analysis is also critical for the identification of "weak signals" that could indicate a surprise attack. A surprise attack is a game of wits between an "attacker" seeking to launch a surprise attack and a "victim" attempting to gather information about the attacker's intentions (Barnea and Meshulach, 2021: 60-75). In this game, the ability to discern "weak signals," often fragmented and ambiguous, is crucial to anticipate enemy moves. This analytical skill requires creativity, original thinking and initiative to construct pre-emptive scenarios, and often involves the study of new and unfamiliar environments. As an NRC study mentions[3] , a good analyst can help his or her clients identify the questions they should have asked, implying an active role in shaping the intelligence agenda.

Cognitive biases and organizational constraints can hinder effective analysis. Analysts often face ambiguous information and must deal with their own biases and assumptions (Kam, 2004: 189-207). Analysis is affected by the need for rapid decision making in groups that may be influenced by leaders or other dominant members. In addition, decision makers may simplify intelligence assessments, which can lead to overlooking important details. The tendency of analysts to be cautious in their predictions and to seek consensus can lead to ambiguities that dilute the strength of their conclusions. The need to give a clear conclusion can lead to the loss of important nuances and an unwillingness to take risks in their assessments.

History shows that military surprise is not only a tactical phenomenon, but also a failure of perception. The real prevention of surprise attack lies not in the infinite accumulation of data, but in the ability to analyze it flexibly and critically (Tetlock and Gardner, 2015: 75-89). The key, therefore, is not only to obtain information, but to understand it before it is too late.

This "too late" materializes with tragic regularity. Fifty years after the trauma of Yom Kippur, Israel has once again suffered its own strategic phantom: the inability to convert available information into decisive action. As Israeli soldiers watched, transfixed, the mass infiltration of Hamas militiamen on October 7, 2023, we witnessed not a failure of intelligence gathering, but the contemporary manifestation of what Bar-Joseph called "the trap of observation without action" (Bar-Joseph, 2005:142-144). The real surprise did not lie in the absence of information, but in the incomprehensible disconnect between ultramodern surveillance systems and decision-making mechanisms anchored in bureaucracies of the last century. This dissociation between knowledge and action demonstrates that technological sophistication, far from guaranteeing security, can generate dangerous complacency when the chain of command lacks protocols that turn analysis into an immediate operational imperative.

Analysis must be transmuted into a mandate. Intelligence that does not catalyze action is mere academic contemplation of disaster. Advanced warning systems lacking automatic triggering mechanisms are vulnerable to institutional paralysis

3 National Research Council (2011). Intelligence Analysis: Behavioral and Social Scientific Foundations. B. Fischhoff & C. Chauvin (Eds.). Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security. The National Academies Press.

(Wirtz, 2004:12-15), a lesson that in 1973 failed to impress itself on Israeli strategic consciousness. To break this inertia, it is necessary to revolutionize the decision-making architecture by creating predetermined thresholds of action where certain critical indicators trigger immediate response protocols, circumventing traditional hierarchies. The October tragedy is evidence that the democratization of decision-making capacity at tactical levels, particularly when information is available in real time, is not an academic luxury but a strategic imperative. Ultimately, intelligence analysis only serves its true purpose when it transcends the informational sphere to become an inescapable catalyst for defensive action.

5 The real tragedy: the loss of the ability to be surprised

In the labyrinth of warfare, where strategy and technology are intertwined, the illusion of controlling the future through information can become a trap. The notion of the "end of surprise" in the military realm should not be interpreted as the eradication of the unexpected, but as the urgent need to cultivate a vigilant mindset. For, despite the apparent omnipresence of information and technological advances, history teaches us that complacency and the loss of the ability to surprise us are the perfect breeding ground for vulnerability.

The root of surprise is nurtured by our own inattention. Often, the abundance of data blinds us, leading us to ignore the signs that warn us of impending danger. Victims of surprise attacks lacked not information, but the ability to interpret it correctly (Kam, 2004: 215-230). Familiarity with routines, complacency and our tendency to reject what we consider improbable make us vulnerable. In a world where information is constantly flowing, the real threat lies in our own inability to pay attention to warning signs.

This interpretative incapacity reveals a deeper and more problematic dimension: the blurring of responsibilities in the analytical-decisional chain. When everyone observes the anomaly, but no one acts, we face not merely a technical failure, but a moral collapse of the security system. "Ambiguity in the attribution of responsibility is itself a lethal vulnerability that adversaries can deliberately exploit" (Bar-Joseph, 2005: 187-189). Decision-making in environments of high uncertainty requires a rigorous distinction between the responsibility of the analyst (to alert with forcefulness proportional to the seriousness of the indications, even if these are fragmentary) and that of the decision-maker (to act decisively with incomplete information when the risks of inaction outweigh those of an excessive response). The complicit silence in the face of this confusion of roles has allowed entire organizations to come to a standstill at critical moments, with each actor taking refuge in the bureaucratic comfort zone of non-responsibility.

The supposed neutrality of inaction is perhaps the most dangerous fallacy in the field of strategic security: the decision not to decide is, paradoxically, the most definitive decision, since it hands the initiative completely to the adversary (Fischhoff and Chauvin, 2011:118-120). This perspective requires revolutionizing our institutional

frameworks, establishing protocols where the responsibility to act in the face of critical indications is not merely an option. Without this catalyzing element that transforms analysis into decisive action, our sophisticated surveillance systems will be no more than passive witnesses, documenting with technical precision but without operational consequence, the next disaster that could have been avoided.

On the attacker's side, the enemy's secrecy sometimes persists as a difficult obstacle to overcome. Despite the transparency of the information age, there are gray areas where adversaries can operate with stealth. A modern example of this is the design of submarine propellers, which have evolved to reduce their acoustic signature and avoid detection. In a world where information seems to be available to all, the reality is that there are operations and capabilities that still elude our knowledge.

History shows that technological evolution is cyclical: at certain moments, systems designed to avoid surprise outperform those that seek to generate it, but later, the situation is reversed (Kam, 2004: 231-246). Military progress does not follow a straight line, but a process of constant adaptation between offensive and defensive (Luttwak, 1987: 212-229). This was the case with the development of radar in World War II. It initially gave the Allies an advantage in detecting enemy bombers but later prompted the creation of stealth aircraft to evade detection. Thus, technological innovation, in its quest for advantage, can also generate new sources of surprise.

In this context, the assumption of an "end of surprise" is, at best, a dangerous fallacy. It is not a question of the eradication of surprise, but of the need to maintain an attitude of continuous vigilance. It is therefore vital to make a critical analysis of available information, to pay attention to subtle signals and to be aware of our own cognitive limitations. The false sense of security, the enemy's ability to conceal his plans and the technological evolution that generates new surprises are factors that ensure that surprise remains an unavoidable element in modern warfare. The real challenge lies in our ability to prepare for the unexpected while maintaining our capacity for wonder and humility in the face of the unknown.

6 Conclusion: end of surprise or evolution of uncertainty?

History shows that surprise has never depended exclusively on a lack of information, but on the human inability to correctly interpret the environment. Over time, technological innovations have reduced the scope for traditional surprise attacks but have not eliminated the uncertainty factor in warfare. Surprise does not disappear with information, but is transformed, exploiting failures of perception, overconfidence and errors in strategic analysis (Betts, 1982: 250-268).

Today, global surveillance and massive data analysis have changed the dynamics of military surprise but have not eradicated it. Warfare remains an environment of high uncertainty, where human ingenuity and adaptability continue to play a crucial role (Freedman, 2022: 398-415). Surprise is no longer based solely on physical stealth, but on the manipulation of perception, strategic deception, and the exploitation of cognitive vulnerabilities.

When information sources are deliberately contaminated with false or manipulated elements, analysts face the challenge of filtering the surrounding noise and distinguishing the truthful from the misleading. In this context, massive information gathering ceases to be a guarantee of knowledge and can instead become a weapon of mass disorientation. History has shown that misinterpreted intelligence or intelligence based on false premises can lead to catastrophic military and geopolitical decisions. Therefore, the key to avoiding surprise in the contemporary world lies not only in the amount of information available, but in the ability to evaluate it in a critical and structured manner.

As Tetlock and Gardner (2015) point out, information overload without rigorous analysis can be as dangerous as the absence of data. Without an adequate analytical methodology, information saturation can generate strategic paralysis or, worse, decisions based on incorrect premises. In this sense, intelligence analysis becomes the true pillar on which strategic security must be built, allowing to convert the chaotic flow of data into actionable and useful information for decision making.

Therefore, we are not facing the end of surprise, but rather its transformation. The question is not whether surprise will disappear, but how it will continue to adapt to a world where information is more accessible than ever, but the interpretation of that information remains the weakest link. As Liddell Hart (1954: 165) stated, "the best surprise is not that which the enemy does not see coming, but that which he sees coming too late to react".

Bibliography

Allen, G. C. and Chan, T. (2017) Artificial Intelligence and National Security. Cambridge, MA: Belfer Center for Science and International Affairs.

Aznar Montesinos, F. (2021) 'El espacio exterior, una nueva dimensión de la Seguridad', Documento de análisis, 10/2021, Instituto Español de Estudios Estratégicos (IEEE).

Bar-Joseph, U. (2013) The Watchman Fell Asleep: The Surprise of Yom Kippur and Its Sources. Albany: State University of New York Press.

Barnea, A. (2005) 'Link Analysis as a Tool for Competitive Intelligence', Competitive Intelligence Magazine, 10(4).

Barnea, A. (2018) 'Challenging the "Lone Wolf" Phenomenon in an Era of Information Overload', International Journal of Intelligence and CounterIntelligence, 31(2).

Barnea, A. and Meshulach, A. (2021) 'Forecasting for Intelligence Analysis: Scenarios to Abort Strategic Surprise', Intelligence and National Security, 36(2).

Behr, I., Reding, A., Edwards, C. and Gribbon, L. (2013) 'Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism', RAND Europe.

Benkler, Y., Faris, R. and Roberts, H. (2018) Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford: Oxford University Press.

Berger, J. M. and Morgan, J. (2015) 'The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter', The Brookings Project on U.S. Relations with the Islamic World, 3(20).

Betts, R. K. (1982) Surprise Attack: Lessons for Defense Planning. Washington, D.C.: Brookings Institution Press.

Boghardt, T. (2009) 'Operation INFEKTION: Soviet Bloc Intelligence and the AIDS Disinformation Campaign', Studies in Intelligence, 53(4).

Borum, R. (2004). "Psychology of terrorism". University of South Florida.

Chesney, R. and Citron, D. (2019) 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', California Law Review, 107.

Clausewitz, K. von (1832) On War. Princeton: Princeton University Press.

DARPA (2017) 'Deep Exploration and Filtering of Text (DEFT) Program', available on the official DARPA website.

European Commission (2020) Tackling Online Disinformation: A European Approach. Luxembourg: Publications Office of the European Union.

European Space Agency (2020) 'SAR Imaging of Electronic Warfare Activities in Conflict Zones', Technical Report Series, ESA-TR-2020-03.

Ferrara, E., Varol, O., Davis, C., Menczer, F. and Flammini, A. (2016) 'The Rise of Social Bots', Communications of the ACM, 59(7).

Fingar, T. (2011) Reducing Uncertainty: Intelligence Analysis and National Security. Stanford: Stanford University Press.

Freedman, L. (2022) Command: The Politics of Military Operations from Korea to Ukraine. London: Allen Lane.

Futter, A. (2018) Hacking the Bomb: Cyber Threats and Nuclear Weapons. Georgetown University Press.

Galeotti, M. (2017) Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right. Rome: NATO Defense College.

Gannon, K. (2021) The Fall of Kabul: Intelligence Miscalculations and Strategic Errors. Washington, D.C.: The Atlantic Council.

Gorodetsky, G. (1999) Grand Delusion: Stalin and the German Invasion of Russia. Yale University Press.

Handel, M. (1984) 'Intelligence and the Problem of Strategic Surprise', Journal of Strategic Studies, 7(3).

Heuer, R. J. (1999) Psychology of Intelligence Analysis. Washington, D.C.: CIA Center for the Study of Intelligence.

Heuer, R. J. and Pherson, R. H. (2010) Structured Analytic Techniques for Intelligence Analysis. Washington, D.C.: CQ Press.

Hill, F. and Gaddy, C. G. (2015) Mr. Putin: Operative in the Kremlin. Washington, D.C.: Brookings Institution Press.

Holt, T. (1978) The Deceivers: Allied Military Deception in the Second World War. New York: Scribner.

International Maritime Organization (2021) 'Shipping Report 2021'. London: IMO.

Jervis, R. (1976) Perception and Misperception in International Politics. Princeton University Press.

Kahneman, D. and Renshon, J. (2007) 'Why Hawks Win', Foreign Policy, 158.

Kam, E. (2004) Surprise Attack: The Victim's Perspective, With a New Preface. Cambridge, MA: Harvard University Press.

Kemp, R. S. (2014) 'The Nonproliferation Emperor Has No Clothes: The Gas Centrifuge, Supply-Side Controls, and the Future of Nuclear Proliferation', International Security, 38(4).

Levy, J. S. (1994) 'Learning and Foreign Policy: Sweeping a Conceptual Minefield', International Organization, 48(2).

Lewandowsky, S., Ecker, U. K. H. and Cook, J. (2021) 'Misinformation and Its Correction: Cognitive Mechanisms and Recommendations for Mass Communication', Psychological Science in the Public Interest, 22(3).

Liddell Hart, B. H. (1954) Strategy. New York: Praeger.

Lucas, E. and Pomerantsev, P. (2016) Winning the Information War: Techniques and Counter-strategies to Combat Russian Propaganda in Europe. Washington, D.C.: Center for European Policy Analysis.

Luttwak, E. (1987) Strategy: The Logic of War and Peace. Cambridge, MA: Harvard University Press.

McGrew, S., Breakstone, J., Ortega, T., Smith, M., and Wineburg, S. (2018) 'Can Students Evaluate Online Sources? Learning From Assessments of Civic Online Reasoning', Theory & Research in Social Education, 46(2).

National Research Council (2011) Intelligence Analysis: Behavioral and Social Scientific Foundations. B. Fischhoff & C. Chauvin (Eds.). The National Academies Press.

Oreskes, N. and Conway, E. M. (2010) Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming. New York: Bloomsbury Press.

Papathanasiou, K., Boutsi, A. and Filippidis, P. (2019) 'Detection and Classification of Electronic Warfare Signals Using Satellite Remote Sensing', IEEE Transactions on Geoscience and Remote Sensing, 57(3).

Paredes, M. and Oliveira, J. (2023). "Emerging technologies and asymmetric threats in the maritime environment."

Pellerin, C. (2017) 'Project Maven to Deploy Computer Algorithms to War Zone by Year's End', DoD News, 21 July 2017.

Pelton, J. N. and Madry, S. (2020) 'Introduction to the Small Satellite Revolution and Its Many Implications', in Handbook of Small Satellites.

Perry, W. J. and Carter, A. B. (1999) Preventive Defense: A New Security Strategy for America. Washington, D.C.: Brookings Institution Press.

Post, J. M. (2003) The Psychological Assessment of Political Leaders. Ann Arbor: University of Michigan Press.

Preston, P. (2012) The Spanish Holocaust: Inquisition and Extermination in Twentieth-Century Spain. London: HarperPress.

Renshon, J. (2021) 'Psychological Approaches to International Relations', in Oxford Research Encyclopedia of Politics.

Rid, T. (2020) Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux.

Schmidt, E. (2020) The Age of AI: And Our Human Future. Little, Brown and Company.

Sun Tzu (500 B.C.) The art of war. Barcelona: Ediciones Obelisco, 2019.

Taddeo, M. and Floridi, L. (2018) 'How AI can be a force for good', Science, 361(6404).

Tetlock, P. and Gardner, D. (2015) Superforecasting: The Art and Science of Prediction. New York: Crown.

Union of Concerned Scientists (2023) 'UCS Satellite Database', Cambridge, MA.

Van Creveld, M. (1991) The Transformation of War. New York: Free Press.

Weeden, B. and Samson, V. (2022) Global Counterspace Capability: An Open Source Assessment. Washington, D.C.: Secure World Foundation.

Wirtz, J. J. (2004). Miscalculation, Surprise and American Intelligence after the Cold War. International Journal of Intelligence and CounterIntelligence, 15(1), 1-19.

Wohlstetter, R. (1962) Pearl Harbor: Warning and Decision. Stanford University Press.

Work, R. (2017) 'Establishment of the Algorithmic Warfare Cross-Functional Team (Project Maven)', Department of Defense Memorandum, 26 April 2017.

Zwitter, A. (2015). "Anticipatory intelligence and strategic surprise prevention".

Article received: January 30, 2025
Article accepted: May 13, 2025