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

*Pau Muñoz Pairet*
*IT engineer and political scientist. PhD in Strategic Studies from the University of Salamanca. Intelligence analyst*

*Email: munyoz.15@gmail.com*

# *The doctrine of the great powers in information warfare*

**Abstract**

Information warfare is a type of conflict that transcends the traditional realm of armed confrontation. The struggle within the information domain has persisted throughout human history, evolving with every advancement in information management technologies, from parchment to the internet. Through a comparative analysis, this paper focuses on the doctrinal vision and approach of the three current major powers: the United States, China, and Russia. Given their advanced media and technological capabilities, these powers emerge as dominant protagonists in this informational confrontation arena. Similarly, their status in the international system, from which a vast array of opposing interests arises, places them in a perpetually latent conflict scenario. Hence, they provide the most substantial base of examples and resources for the study of this phenomenon. By examining their recent history, as well as their doctrinal documents and primary academic contributions, we come to understand not only their strategies and tactics but also the dynamics of competition and the evolution of information warfare in the contemporary context.

**Keywords**

Cognitive warfare, Cyber warfare, Propaganda, Realism, Foreign policy.

**Cite this article:**

Muñoz Pairet, Pau (2024). The doctrine of the great powers in Information Warfare. Journal of the Spanish Institute for Strategic Studies. N. 23, pp. 281-312.

## 1. Introduction

The premise information is power has consistently resonated throughout human history. Throughout the various periods of human history, information management has dominated political dynamics in numerous arenas: influencing tactics, operations and strategies around the world. Its historical influence has been and continues to be far-reaching, manifesting itself both in times of conflict and in times of peace. During periods of war, information has served both as a weapon and as a battlefield, being used for deception, the implementation of camouflage or decoys, the spread of rumours and the interception of enemy communications. In peacetime, it has represented the cornerstone of espionage, a key tool for political manipulation in its various forms. In this respect, information control has been used both defensively and offensively.

Competition for control of the information domain is not a recent phenomenon. In fact, it has been the subject of analysis and documentation in multiple cultures throughout history; from the teachings of Sun Tzu in China and Kautilya in India to the reflections of Xenophon and Thucydides in classical Greece. The same importance can be seen in Rome, in Frontinus› *Stratagemata* and, centuries later, in Machiavelli›s *The Prince*. These works, among many others, underlined the intrinsic value of information and how its mastery and management have influenced the strategic culture of different nations over time (Gilpin, 1984).

As technology advanced, its impact on information management became evident. From the invention of the printing press, through the advent of radio and more recently, the proliferation of the Internet, each technical innovation was quickly adopted and adapted to serve the information warfare. Not only technological innovations, but also social developments, particularly the Industrial Revolution, have played a fundamental role in structuring and developing the strategies and tactics of this type of conflict. These developments motivated armies and intelligence services of various nations to develop and strengthen their Information Warfare capabilities. As a result, these methods and techniques are not only employed in armed conflicts but are also central to covert actions and the dissemination of state propaganda.

Contemporary information warfare is in a phase of consolidation. Since the Second World War (WWII) it has undergone significant development, which has increased in recent decades, and is now recognised as an autonomous form of conflict, worthy of study and analysis in its own right. Its relevance is such that it often becomes the core of military operations and is essential to modern political power projection strategies.

Although information warfare is a global phenomenon involving multiple state and non-state actors, the great powers currently dominate this arena with the greatest intensity. Naturally, information warfare is a complex phenomenon, which requires both solid intelligence systems, a particular capacity for global influence and a strongly developed technological sector. Thus, the dominance of the great powers over this

mode of warfare is largely due to their advanced media and technological sectors. Not only do these powers have the capabilities, but also clashing interests that drive them to compete actively in this field, with the overriding goal of expanding their influence globally.

In this article we focus on the study of Information Warfare from the perspective of the three great powers of the international system: the United States, China, and Russia. Through a comparative analysis, we examine their doctrinal approaches. Beyond understanding their capabilities and potential in the field of information warfare, this research allows us to study their competitive dynamics, as well as the evolution of this mode of warfare throughout recent history.

To carry out the analysis, we have taken into consideration the main doctrinal documents available in official publications. Similarly, the contributions and analyses of leading intellectuals and military think tanks in each of these nations have been taken into consideration.

## 2. War in the information domain

Information warfare is defined as a mode of warfare that involves the manipulation, distribution and, occasionally, denial of information. Its main purpose is to gain a competitive advantage over the opponent, while simultaneously protecting one›s own information systems (Libicki, 1995). The aim is to influence the opponent›s decisions, behaviour, perceptions and capabilities. To achieve this, a wide spectrum of tools and tactics are employed, ranging from traditional ones, such as propaganda and disinformation, to more contemporary ones, such as cyber operations and electronic warfare (Libicki, 2017).

The definition encompasses both traditional, primarily cognitive-based methods of information warfare, such as propaganda, and more recent methods, such as technical operations in cyberspace. This mode of warfare can manifest itself in a variety of contexts, whether in peacetime or during armed conflict, and can be executed by both state and non-state actors.

Conflict in the information space cuts across all aspects of information management. It focuses not only on the channels of communication, but also on those who send and receive the information, as well as on the content of the message itself. Within this approach, the human being is recognised as a vital actor, playing simultaneously the roles of sender and receiver within the vast information ecosystem. Thus, when we speak of information warfare, we are referring both to operations that attack or defend the cognitive aspect of information - such as disinformation and propaganda - and to those that focus on its technological dimension, such as electronic warfare, cyberespionage and cyberwarfare (Aro, 2016; Robinson M. K., 2015; Sampanis, 2024).

Beyond the use of technological innovations, this mode of combat is characterised by its versatility and adaptability. Thus, it can manifest itself subtly in times of peace

between nations, becoming evident through activities such as espionage or political influence. In a context of open warfare, it has the capacity to escalate and adapt quickly to more belligerent contexts. In such open conflict scenarios, it can escalate to more aggressive tactics, such as electronic warfare, mass dissemination of disinformation or even cyber-attacks with purely sabotage objectives. All operations that escalate from a pre-existing base built before conventional warfare, on already established tactics.

Once the conflict has ceased, information warfare operations may decrease in intensity, adapting to the new post-war scenario. However, these operations never disappear completely; they are simply transformed and adapted according to circumstances.

Thus, this adaptive approach to information warfare makes it one of the main tools in the service of hybrid warfare operations, a mode which combines conventional and unconventional tactics in the same military arena (Hoffman, 2007). In this context, this phenomenon aligns perfectly with the concept of grey zone actions, operations that fall between peace and outright conflict, and which seek to exploit ambiguities and gaps in international regulations and norms (Votel, 2016; Liu, 2024).

## 3. The great powers in information warfare

To fully understand the dynamics in the international system, characterised by its typically anarchic nature, we turn to the main theories that have attempted to explain such relations. Among the many existing currents, the realist perspective emerges as the predominant one in the contemporary study of international *r*elations (IR). Realism is not monolithic and presents significant sub-currents, among which we can identify neoclassical realism, structuralist realism -also known as defensive realism, represented by theorists such as Waltz-, and offensive realism, whose main figure is Mearsheimer (Waltz, 2018; Mearsheimer, 2001).

The lens of offensive realism stands out as offering a particularly enriching conceptual tool for dealing with information warfare between the great powers. In this light, such a war is not an anomaly, but an inevitable and persistent component of the international power game.

Within this theoretical framework and backed by the consensus in the field of international *r*elations, Mearsheimer conceptualises great powers as those states equipped with military forces robust enough to not only defend their territory but also to project power beyond their borders (Mearsheimer, 2001). They have nuclear capabilities and an advanced technological environment. Moreover, their resources and economic strength make them remarkably self-sufficient. These powers are also characterised by a high degree of political autonomy and possess distinctive political and cultural systems that have the potential to be promoted or defended internationally as tools of influence. Naturally, this combination of factors fuels its geopolitical ambition.

In the same vein, it should be stressed that if any of these great powers manages to consolidate hegemony at the regional level, it can be categorised as a superpower or hegemonic power. This designation has profound implications for the balance of the international system and how these entities interact with their counterparts.

Today, Russia, China and the United States dominate the global stage as great powers. The United States, in turn, plays a leading role in the system, established as the only superpower in the international system. Despite the current US regional hegemony, we cannot ignore China´s growing presence in the system and its stated intention to reach a similar position in the coming years.

Thus, the offensive realism approach, as outlined by Mearsheimer, suggests that, in an anarchic international system, these great powers, in their eagerness to ensure their own security, are inclined to maximise their power (Mearsheimer, 2001). This expansion of power, if conditions are right, can materialise through direct military intervention. The underlying logic suggests that, in the long run, conflict between these powers becomes more likely, especially when we are in a context of unbalanced multipolarity. China´s recent growth signals that the international system is in transition towards this type of configuration (Mearsheimer, 2021). In this sense, the United States, in accordance with the postulates of this approach in international *r*elations, is in the process of adapting its foreign policy to face the competition for power in the Indo-Pacific (Perez, 2023).

In the struggle for global hegemony, confrontation between the great powers is practically guaranteed. The establishment and consolidation of hegemony involves not only military or economic dominance, but also decisive political and cultural influence on the rest of the system. It is therefore common for these powers to collide as they try to exert their influence in similar regions or attempt to undermine the regional dominance of their rivals. Information warfare emerges in this context as an essential strategic tool. Its advantage is that it tends to carry minimal political costs, but with the capacity to escalate into more aggressive and extensive operations should it lead to a traditional military confrontation (Harknett, 1996). Given these dynamics, information warfare is not only likely, but inevitable in the global arena. The relevance of examining this phenomenon from a great power perspective is indisputable. These nations, given their vast resource pool, strategic interests and capacity for self-sufficiency, are in an unparalleled position to formulate and dictate specific doctrines. In addition, they have the ability and means to develop clear techniques and strategies in the field of information warfare, thus reflecting a distinctive and characteristic approach.

To investigate this phenomenon, it is essential to approach it through doctrinal analysis of these preponderant powers. An effective methodology for this study involves the close examination of official documents issued by these powers.

Thus, in order to practically study a country›s doctrine on information warfare, we shall rely on the analysis of the main official documents in a multi-level strategy

combining the analysis of the historical context with the legal and especially the military doctrine.

Before starting the doctrinal analysis, we should bear in mind the historical context of the country, both in terms of its internal politics and especially in terms of its interaction with the other powers, as its historical facts, legends and myths can often be instrumentalised in information warfare, and its historical tendency will naturally give us a general idea of its mode of action. When analysing a country›s doctrine, we will first look at the official doctrinal documents on the subject, often issued by the respective Ministry of Defence, National Security Council or equivalent high-level organisation. These documents will be a combination of the country›s historical context, its political idiosyncrasies, national interest and capabilities. Where official doctrinal documents are available for the particular period of study, the analysis can be largely derived from them. In studying US doctrine, we will therefore look at the *Joint Doctrine Publications* and the various iterations of the National Security Strategy, documents that either cover the official US view on specific information warfare matters such as psychological warfare or cyberwarfare, or the country›s general strategy in which these aspects are included. With regard to the study of China, we will look at the various white papers, their discussion of National Defence, the Defence Policy documents, as well as the various specific military manuals on these subjects. Finally, in the case of Russia, we will study the Russian Federation›s Military Doctrine and the different iterations of the National Security Concept, complementing them with the National Security and Foreign Policy Strategies periodically released by the office of the president.

At the second level of analysis, we find the set of legal instruments and executive resolutions relating to the different sub-domains of information warfare. Although said documents do not establish a doctrine after their publication, as the resolutions affect partial developments and the laws can be interpreted or applied in different ways, they do allow us to establish the country›s capabilities and possibilities when it comes to confronting this domain.

The third level of analysis will be composed of the collection of publications issued by the country›s main centres of thought on military, security or strategic studies in general. While the documents published in said forums pave the way for the establishment of formal doctrines, their academic and prospective nature means that the work within them is often considerably more advanced to the practical reality of the country. It is therefore very common to see how works of analysis and reflection on matters related to information warfare published in the main journals and strategic forums end up giving rise to the establishment or simple formalisation of national doctrines. In the United States we will look largely at the work published in institutions such as the Rand Corporation, the *Military Review*. In Russia we can look at the content of publications such as Военное Обозрение (*Military Review*) and Военнно-промышленнный курьер (*Military-Industrial Post*). In China we will look at the 解放军报 (*PLA Daily*), as well as the 中国国防报 (*National Defence Newspaper*).

Finally, we can supplement the analysis with a study of known information operations, the structure of the armed forces and the main ideological currents in international politics in the respective countries, as well as taking into account the country›s own position in the international system and its status in terms of the development of its media and scientific-technical systems, since it is through these systems that it will be able to build its capabilities.

Therefore, when carrying out this analysis, we have relied on the study of these documents through the methodology outlined above.

### *3.1. The US doctrine*

Information warfare, as we know it today, originated as a term used in US military circles during the 1980s. However, its essence and practical application go even further back in time. It was after the Gulf War that this term acquired the essential importance it retains today, highlighting the relevance of information and disinformation in the field of operations.

Thus, if we trace the origins of organised US implementation of information warfare tactics, we find that they date back to the early decades of the last century. It was during this period that theorists such as Lasswell and Lippman began to develop concepts and strategies around the power of information (Laswell, 1948; Lippman, 1946). His work provided the basis for establishing a theoretical and practical framework within which the United States could begin to operate. Lippman himself played a central role in helping to found and direct the public opinion committee, articulating much of American war propaganda in World War II around innovative concepts, from radio to the use of humorous cartoons (Ruiz, 2018).

At a military level, we can trace the initial efforts in US information warfare to World War II. During World War II and the Cold War, the United States intensified its tactics in this field. During this time, it incorporated specific tactics and strategies to dominate the media landscape. Hollywood produced films that favoured American values and countered adversarial propaganda, while the US government promoted propaganda efforts through agencies such as the Committee of Public Opinion and the creation of propaganda agents such as the Four minutes men.

Beyond mere internal propaganda, the military tactics of the era incorporated elements of deception and camouflage, reaching new heights of complexity. Notable examples include the use of inflatable tanks, bonfires or loudspeakers, as well as other simulations to deceive the enemy about the location and size of Allied forces. The notorious Operation Mincemeat, in turn, is another classic example of strategic deception where the body of a dead man was used to transmit false information to the Nazis.

The field of electronic warfare underwent a major revolution during this period. Beach jumper units were established by the US Navy to conduct deception operations,

based primarily on jamming and the deployment of electronic decoys. Similarly, interception and protection of information also became key areas, as seen in the collaboration between the Allies to decipher Nazi codes and in the use of Navajo for communications, an indigenous language used as a virtually unbreakable code at the time.

During the advance of the Cold War in the 1960s and 1970s, information warfare was central between the United States and USSR focusing on espionage and ideology. The US and its allies debated ideologically against the USSR and communism, seeking to promote democratic and capitalist values. To this end, the US used media, educational programmes and support for pro-democracy organisations, acting both overtly and covertly. Initiatives such as Voice of America and Radio Free Europe/Radio Liberty broadcasted news in censored areas, while documents such as the Church report revealed covert Central Intelligence Agency (CIA) tactics in information warfare. In education, programmes such as Fullbright, which focused on educational and cultural exchanges, sought to project democratic values and practices abroad by ensuring US influence through soft power (Nye, 1990).

However, it was not all directed outwards; Operation CHAOS, under President Johnson, emerged in the context of the Vietnam War to monitor domestic anti-war groups, reflecting the growing concern about the effects of information warfare within the country›s own borders. This concern was also evident during the war against the Viet Cong itself, where psychological operations, such as Wandering Soul, were based on a deep understanding of Vietnamese culture, and there was a constant attempt to manage and control the narrative presented by the press.

In the 1980s, with Ronald Reagan as president, the US intensified its ideological stance. In 1982, the Reagan administration sought to strengthen the infrastructure of democracy by investing more in prodemocracy media and organisations. In 1983, the National Endowment for Democracy (NED) was founded with an initial budget of $31.3 million to support democracy, press freedom and human rights in communist-influenced areas.

In turn, during this period, information warfare took on a more strategic nature. The Strategic Defence Initiative demoralised the USSR, labelled as the evil empire by Reagan, in its competition with the North Atlantic Treaty Organisation. In Latin America, Radio and Television Martí were created in 1985 and 1990 to influence Cuba, and the US supported the Contras in Nicaragua, reaffirming its anti-communist stance, showing that, in information warfare, ideological battles influenced history as much as military power.

The 1990s and 2000s brought with them new challenges arising from the technical and professional sophistication that enabled the launch of 24-hour news channels and the subsequent emergence of internet communication. During the 1990s, the CNN effect and the televised war demonstrated the power of the media to influence public opinion essential to justifying US foreign policy (Robinson, 1999). This was particularly evident during the Gulf War and the successive

Balkan Wars, where the country›s own public opinion played a key role in facilitating military intervention. Thus, in response to the growing importance of public perception in the international context, successive US administrations began to move from psychological action to strategic communication. An approach to the direct manipulation or influence of public opinion to gain support for military and political actions abroad was observed. This approach integrated the media as an essential tool in information warfare, using real-time coverage and intensive reporting to foster narratives that aligned public opinion with the government›s foreign policy objectives (Robinson, 1999).

At the same time, technological transition, represented by the expansion of the internet and digitalisation, demanded a rethinking of information security. The Bush and Clinton administrations initiated both defensive and offensive efforts in cyberspace. With resolutions, such as National Security Directive 42, and the formation of working groups, the US sought to strengthen its information infrastructure. Amidst these technical advances, a recognition of the need for a more coherent theoretical framework emerged. Libicki (1995) Johnson, (2004) among others, worked on the disambiguation and structuring of the concept of information warfare, generating a comprehensive framework of understanding, not only from a technical angle, but also from a cognitive and psychological one.

Thus, the turn of the millennium saw a rapid formalisation of these ideas. Documents such as Joint Vision 2010 and the Joint Doctrine for Information Operations emerged as benchmarks in Information Warfare. In addition, the Joint Publications series detailed specific operations, from electronic warfare to cyberspace operations.

The attacks of September 11, 2001 reshaped the perception of security in the United States. Information warfare tactics were no longer just tools in the struggle of nation-states, but also of non-state actors (Soriano, 2018). In the contemporary, post-2018 scenario, the U.S. Department of Defence has recognised the importance of cognitive warfare. The current emphasis is on strategic communication (STRATCOM), moving away from pure psychological manipulation towards an attempt at positive and explanatory influence, where the justification of military actions takes centre stage.

Today, as far as information warfare is concerned, while there is no official US government definition, leading military analysts and officials generally conceptualise it as a strategy or planning process to achieve objectives and goals of national interest, for the use and management of information to gain a competitive advantage, including both defensive and offensive operations. In this respect, (information) operations, developed extensively in previous decades, represent the link that connects strategic objectives with tactics, techniques and procedures. Beyond the lack of a unified definition, it is worth noting that various organisations and experts in the country have contributed their own perspectives on the subject and maintain them as a doctrinal framework, with the Department of Defense (DoD) being the most relevant organisation. The DoD has thus conceptualised information warfare since the beginning of the century as an interrelationship between physical information systems and information itself (Understanding Gray zone warfare from

multiple perspectives., 2023). Information warfare would focus on affecting the (military) decision-making process by attacking physical information systems or the information itself.

It is important to understand that, according to the US doctrinal approach, these activities naturally take place within the information domain, which comprises three main dimensions: physical, communicative or information and cognitive. In the digital age in which we are immersed, all instruments of national power can be projected and employed in this new environment, including by non-military elements of government, responding to a common strategy (The White House, 2022). As for the cognitive-based aspect of information warfare, three main categories have been identified in the US; three ways in which information can be manipulated or biased, namely propaganda, misinformation, focused on misleading the enemy, and disinformation, or biased information with possibly false parts focused on deception and manipulation (ODNI, 2023). The current US strategic approach in this regard focuses on the dissemination of accurate and truthful information combined with the use of propaganda to influence public opinion in enemy societies (USA-JCS, 2022). To this end, the US government, through various national initiatives, routinely sponsors fake news identification technologies, news verification agencies and similar entities. This modus operandi is applied both internally within the country, as a defensive measure, and externally, seeking to neutralise enemy narratives, replacing them with its own propaganda, through favourable media and official outlets such as Voice of America and the like.

However, unlike the autocratic powers discussed below, the US strives to apply information warfare tactics in an offensive but also defensive manner, where ethics are important, and freedom of the press must be respected. Similarly, the complex network of agencies and units linked to the information warfare in the US as well as the democratic nature of the country, makes it particularly difficult to carry out certain types of actions in a coordinated and effective manner, something that autocratic powers do not suffer from.

In terms of actions in cyberspace, the US strategy has enormous advantages over its adversaries, due to the strength and scientific-technical sophistication of the military industrial complex, as well as the possibility of establishing agreements and links with strategic companies such as Google, Microsoft or certifying entities linked to encryption systems.

US information warfare capabilities are thus organised through a complex network of government agencies, military units and the indispensable support of think tanks and the military-industrial complex. While in the US, influencing and propaganda in favour of its foreign policy can be carried out through a network in which NGOs, strategic companies and even individuals can operate in a, more or less, coordinated manner with government interests, the main capabilities in this area are shared between the Intelligence Services, the Armed Forces and the State Department (ODNI, 2023).

### *3.2. The Russian doctrine*

The Russian approach to information warfare, while not departing from the general approach to the concept, has deep roots in its history. It is worth remembering that Russia›s relationship with the control of information and propaganda in modern times is as old as the Russian Revolution itself. It was during this period that the management of information became particularly important, becoming both a weapon and a battlefield, in a scenario in which the lines between politics and war were becoming increasingly blurred. The rise of the communist party and the triumph of the October Revolution would mark the beginning of a historical tradition in information warfare, allowing for the development of a unique approach.

After the October Revolution of 1917, propaganda became one of the main weapons in the Bolshevik arsenal, being used to legitimise themselves, broaden popular support and consolidate their power through the information space. Posters, leaflets and newspapers with pro-Bolshevik messages were distributed. During the Russian Civil War (1918-1922), propaganda sought to destabilise opponents both inside and outside Russia. Revolutionary fervour spread beyond Russia›s borders, influencing Europe, with the backing of the Communist Party.

After achieving military victories in the war and consolidating its power, the Communist Party, aware of its value, began to articulate a comprehensive strategy for absolute control of the information domain. On the official level, the Bolsheviks began consolidating their control over the media space. Thus, shortly after the October Revolution, they issued the Press Decree, placing restrictions on the non-socialist press, ensuring almost total domination over public discourse. At the same time, the Cheka, the Bolshevik secret police, was set up. Beyond its intelligence work, it played an essential role in spreading the Bolshevik message, especially in the repression of any form of dissent.

As to the handling of information warfare, a central pillar in this propaganda apparatus was Agitprop, established in 1920 (Mally, 2003). As the main propaganda arm of the party, it played a crucial role in promoting communist ideology both inside and outside the USSR. This committee stood out for its great management of the information space, putting creativity and the technologies of the time at the service of propaganda. Clear examples of this can be found in the rosta posters, a series of propaganda posters created by the official news agency Rosta between 1919 and 1922. These posters were pioneers of Russian propaganda strategy and would be used by the party throughout the Cold War, being equivalent to the current memes that are so relevant across online social networks. Similarly, stations such as Radio Moscow became the first instruments of international influence projection in the country.

The Communist International, or Comintern, emerged in 1919 to propagate the Communist Revolution globally, reflecting Russia›s strategy of winning ideological allies against capitalist influences. This organisation, active from 1920 to 1943, put ideology at the service of USSR propaganda and strategy. Their actions were based on

doctrinal documents, such as the 21 Conditions of 1920, which emphasised loyalty to Moscow and violent revolution. The Comintern Programme of 1928 reaffirmed these aims, promoting the dictatorship of the global proletariat.

From its earliest days, the Comintern was resolute in its mission. Its mandate, to fight against bourgeois organisations and to fight for an international soviet republic, revealed its overall revolutionary aim. However, its efforts to catalyse communist revolutions in post-World War I Europe, while passionate, had limited success. They sought to capitalise on discontent in countries such as Germany, especially the fragile Weimar Republic, and Hungary, where a Soviet republic briefly emerged in 1919. However, political and social circumstances did not always favour the emergence of lasting communist regimes. In many of the conflict arenas, communist ideology had to struggle against reactionary movements and local nationalism.

Noting that the Comintern›s results in Europe were not entirely favourable, the organisation shifted its gaze to Asia. Being a continent with vast territories and populations, and where colonial and post-colonial discontent offered opportunities for communism. Thus, its support was instrumental in the founding of the Chinese Communist Party in 1921, which would eventually become one of the most powerful communist forces in the world.

The 1930s would present new challenges for Soviet influence in Europe due to the rise of fascism on the continent. In response, the Comintern adopted a firm anti-fascist stance, urging communist parties to form alliances, known as popular fronts, with other left groups to counter the threat. But geopolitics is always complex, and during the Molotov-Ribbentrop Pact between 1939 and 1941, the Comintern had to adopt a stance of neutrality towards Nazi Germany. This position would change drastically with the German invasion of the USSR in 1941, bringing the Comintern back to the stalwart support of the anti-Nazi resistance in Europe. However, Soviet geostrategic realities in the context of World War II demanded a political flexibility that the Comintern could not manage. In 1943, Stalin dissolved the Comintern, partly as a gesture to his new Western allies. He argued that the Comintern had fulfilled its mission and was no longer needed in the new stage of global politics.

Although the Comintern was disbanded, this did not mean the loss of the USSR›s Information Warfare capabilities, quite the contrary. In parallel to ideological initiatives such as this organisation, the Soviet Union strengthened its intelligence and espionage capabilities. Organisations such as the People›s Commissariat for Internal Affairs of the Soviet Union (Народный комисссариат внутреннних дел СССР, NKVD) and the Central Intelligence Department of the Armed Forces (Главное Разведывательное Управление, GRU) were established, and during the 1920s and 1930s, Moscow created specialised schools to train agents in espionage, counterintelligence, and propaganda techniques. These agents, once trained, were deployed all over the world, becoming the eyes and ears of the Soviet state before, during and (especially) after the war. Later, the NKVD would evolve into the main intelligence body of the Committee for State Security (Комите́т Госуда́рственной Безопа́сности, KGB). In this sense, the Second World War gave way to the Cold War,

a period marked by Information Warfare between the two great blocs. In strictly military terms, information management played a decisive role in the Soviet victory in the East. It was during this period that Soviet military doctrine integrated the use of deception at all levels, giving rise to the term Maskirovka as a doctrinal approach (Keating, 1981), a doctrinal approach, it must be said, which was revived after the Russian resurgence under Putin (Staun, 2023).

During the extended Cold War period, the USSR focused on its confrontation with the Western bloc. Being not only a military but also an ideological and political struggle, the USSR›s tactics ranged from propaganda to covert intelligence. Radio stations such as Radio Moscow and Voice of Russia were vital in this regard, broadcasting Soviet propaganda to global audiences in several languages, and often presenting the world from a pro-Soviet and anti-Western perspective. In the field of covert operations, Soviet intelligence services carried out particularly relevant manoeuvres such as Operation INFEKTION in the 1980s, which spread the unfounded rumour that the HIV/AIDS virus was a creation of the US government (Bates, 2010). They also sponsored magazines such as *New Times* and *World Marxis Review* to disseminate their ideological perspective. During the 1980s, amid rising tensions, the USSR initiated disinformation campaigns that portrayed the United States as the main impediment to world peace, while striving to promote disarmament initiatives that furthered its own interests. These operations, referred to in the KGB doctrine as Active Measures, covered a wide range of tactics aimed at influencing politics and public opinion in other countries. These were not limited to disinformation. The Soviet strategy was broader, focused on seeking change in the political system. In this sense the USSR provided funding, arms, training and propaganda to support communist parties and liberation movements in different parts of the world, in collision, naturally, with the USA (Brantly, 2020).

In this context, the KGB, which was the backbone of these strategies and was primarily responsible for the operations described above, developed numerous manuals that became doctrine. While much of it was classified as secret, examples leaked as *The Science of Disinformation* (Bittman, 1985) in the 1980s detailed techniques and tactics for disinformation operations. These were mainly based on the creation of false stories, the use of fabricated documents, the infiltration of the media, and cooperation with sympathisers and agents abroad (Darczewska, 2015).

Similarly, specialised institutions were set up to train agents in these techniques, becoming experts in information warfare. Over time, Soviet military doctrine, reflected in concepts such as deep war and Maskirovka, underlined the need to use disinformation and deception as crucial tools, both in the information sphere and on the battlefield.

When the USSR disintegrated in 1991, the KGB gave way to new intelligence services in Russia, such as the Federal Security Service of the Russian Federation (Федеральная служба безопасности Росссийской Федерациии, FSB) and the Foreign Intelligence Service (Служба Внешней Разведки, SVR), continuing similar operations in line with Russian foreign policy, inheriting its approach from the Soviet

one. Similarly, the GRU continued its activities, responsible for military intelligence and sabotage operations. Today, these three bodies are central to the design and execution of Russia›s major Information Warfare operations.

The disintegration of the Soviet Union in 1991 marked a turning point in the global geopolitical landscape. Russia, the largest successor state to the USSR, was plunged into a deep political, economic and social crisis. This internal situation had direct consequences on its presence and influence in global affairs. In the years immediately after disintegration, Russia was predominantly focused on its internal affairs, striving to ensure a modicum of stability in a country undergoing radical transformations.

This Russian introspection somewhat overshadowed its information warfare operations. During the 1990s, Russia faced severe financial constraints that affected many sectors, including the information warfare one. There was a significant reduction in funding and prioritisation of such operations, resulting in a virtual paralysis of efforts in this domain for much of the decade. However, the entry into the chaos of the 1990s not only affected Russia›s ability to undertake information warfare operations, but also laid the groundwork for a transformation of the system that would later lead to renewed efforts in this field in the new millennium. It is essential to understand two crucial aspects that emerged in this context.

First, the collapse of the USSR created power vacuums in Russia. These, combined with the economic emergency and the process of accelerated privatisation, facilitated the emergence and consolidation of various non-state actors with great power and influence. This group includes the well-known oligarchs, tycoons who amassed enormous fortunes during this period and who, over time, became major political players. Although these oligarchs occasionally operated on the margins of the state, they possessed significant economic and political power. As a result of their situation, they began to maintain a set of interests that sometimes transcended and even contradicted Russia›s official foreign policy.

Secondly, the temporary fragility of the Russian state in that decade left an open door to foreign influence, especially in the cultural, political, telecommunications and other sectors. In telecommunications, some foreign companies began operating in Russia to connect Russia to the global network, marking the beginning of the internet era in the country. Unlike in nations such as China, where mechanisms for network control and regulation were quickly established, Russia, aspiring to democratisation and under Western influence, did not implement legal frameworks and rigorous technical capabilities to regulate telecommunications until much later. This lack of regulation led to the flourishing of a community of hackers and political commentators (Woolley, 2018), who in subsequent years would play a key role in the evolution of information warfare from the Russian approach.

Similarly, the perceived fragility of the newly formed Russian state in the 1990s not only exposed the country to foreign influence, but also set the stage for the emergence of new political actors. The latter saw rapprochement with the West as an opportunity to consolidate their position and political success. This geopolitical context led to

a series of movements and revolts across the post-Soviet space better known as the Colour Revolutions in the first decades of the 21st century. Said Colour Revolutions refer to a series of political movements that took place in several post-Soviet countries, such as Ukraine, Georgia and Kyrgyzstan, where mass and mostly peaceful protests led to the removal of governments deemed authoritarian or corrupt and their replacement by more pro-Western regimes. For Russian elites, these movements not only represented a challenge to their traditional sphere of influence, but also raised deep concerns about possible foreign interference and the export of Revolutions to Russia itself. This context of revolutions and the geopolitical changes they brought with them generated a sense of alarm and mistrust among the Russian authorities, who interpreted these revolutions as part of a Western-driven hybrid warfare strategy (Guerasimov, 2013).

In the face of this general sense of alarm, the systematic response of Russian elites was to armour the national information space, not only by reinforcing censorship and capacity building, but also at the moral and ideological level. Thus, by establishing a new national narrative reinforced by propaganda capable of unifying the country ideologically, the country would be better shielded against various campaigns of foreign influence, whatever they might be. The elites, thus, found in currents such as Aleksander Duguin›s Eurasianism an ideological basis on which to build a national narrative and thus justify their foreign policy or even go so far as to fight for the hegemony of the narrative against liberal democracy. Duguin himself would highlight the role of propaganda and the establishment of alternative national narratives to Atlanticism in one of his major works; rn Project Eurasia stressed the need to "establish an alternative communication ecosystem to the dominant Atlanticism" (Duguin, 1999).

It is precisely the ideas of thinkers like Duguin that would begin to take shape from 2005 onwards through the progressive establishment of an entire Russian international communication ecosystem. Said system would be headed by the Russia Today channel established that same year, along with other channels and agencies like Sputnik, and would in turn be backed by a wide network of proxy media linked to extremism of all kinds, alternative communicators and social media (Galán, 2023). The application of these new capabilities would allow the Kremlin to begin to contest the Western narrative around the world with particular success in regions with latent anti-imperialist currents and sentiments such as Ibero-America (Miles, 2021). This narrative battle would progressively begin with the launch of media outlets such as RT and would gradually intensify after events such as Euromaidan or the very beginning of the Special Military Operation in Ukraine (Darczewska, 2014).

Similarly, this fear, together with the technological revolution that was redefining the media, accelerated Russia›s interest in developing and consolidating its own doctrine in the field of information warfare, as well as specific capabilities such as military units in the form of information troops or new means of cyber and electronic warfare (Gerasimov, 2016; Lysenko, 2018). This transformation was nurtured by the thinking of Russian academics and military men and translated into a series of guidelines and strategies that were incorporated into official Russian army doctrine (Rumer, 2019).

Once the problem in the information domain had been identified and the first capabilities in the media sector had been built, Russian elites proceeded to transfer this new scenario into a formal doctrine. As the 21st century progressed, and under Vladimir Putin›s administration, this doctrine was both embodied in various official strategic documents and materialised in the construction and application of capabilities, consolidating Russia›s vision of information warfare as a response to the challenges it presented in the international arena.

Russia›s contemporary stance in information warfare is rooted in a number of key strategic documents. The Military Doctrine of the Russian Federation, updated in 2014 (Kremlin.ru, 2010; 2014) while focusing primarily on traditional military defence matters, emphasises the importance of information and stresses the need to safeguard the country›s information sovereignty against external threats that seek to destabilise its sovereignty and territorial integrity. In 2016, the Information Security Strategy of the Russian Federation was adopted (рф, Доктрина информационной безопасности Российской Федерации, 2016) which prioritises information security, identifies threats in the digital sphere and establishes a framework for preserving national information integrity. In the same year, the Foreign Policy Concept of the Russian Federation emphasised the need to use information tools to achieve foreign policy objectives, recognising the conflicts that are projected in the information space (рф, kremlin.ru, 2015-2021) and in its 2023 version it further emphasises defence against "disinformation and the influence of external actors", understanding the defence of the country›s internal information space as a central element in national security and an enabler of foreign policy (kremlin.ru, 2023). On the other hand, while the Russian Federation›s National Counterterrorism Strategy focuses on terrorism, it does not overlook the imperative of combating the spread of extremist ideologies in the information sphere.

This doctrinal framework reflects the Russian idea of Information Warfare as a multifaceted phenomenon, articulated through the military, the intelligence services and the official media, encompassing both cognitive and technical dimensions (Darczewska, 2015). Notorious examples of this stance are Russian actions integrating hacking, leaks, disinformation and propaganda techniques, as evidenced in events such as the intervention in Estonia in 2007 (Ottis, 2008; Sanger, 2016) and the alleged interference in the 2016 US elections. Russia, recognising itself as a persistent target of this information war by the West, adopts a defensive stance that often manifests itself in counterattacks, explaining its behaviour and perspective on the current global stage.

### *3.3. The Chinese doctrine*

China emerges as a player in information warfare, with a less sophisticated doctrinal development than the United States, but with an informal doctrine, solidly embedded in its strategic and military thinking. Although the value of information control has been recognised in China since ancient times, it has been during the last three decades

that the country has undergone a doctrinal revolution, especially after the Gulf War (Cheng, 2011).

The control and manipulation of information has been central to Chinese strategies since the time of Sun Tzu, as illustrated in the *Art of War*, a treatise that emphasises the importance of strategy, intelligence and cunning in combat (Ota, 2014). However, to understand the modern doctrine of Chinese information warfare, we must go back to the second half of the 20th century and the establishment of communism in China.

Thus, with the advent of the communist revolution in 1949, and the establishment of the People›s Republic of China, the importance of information control rose to unprecedented levels. In this context, propaganda became a crucial tool for the promotion and consolidation of communist ideology. However, due to the country›s technological and economic limitations at the time, the technological facet of China´s information warfare did not develop until much later. During this early period, the foundations of the country›s information machinery were laid, with entities such as the Xinhua News Agency and the People›s Daily playing key roles, roles which they still retain today.

The next critical stage in the evolution of information warfare in China was the Cultural Revolution (1966-1976). This decade witnessed an intensification of propaganda, where its main objective was to consolidate the power of the Communist Party of China (CPC). During this time, propaganda was not only omnipresent, but also extremely political. Mass mobilisation and propaganda reached uncontrollable levels, with intense ideological campaigns aimed at eliminating counterrevolutionaries and other enemies of the state. These campaigns took the form of study sessions, infiltration of all sectors of society, activation of youth groups, distribution of written material, and radio broadcasts (Mittler, 2014). The end of this era came with the rise of Deng Xiaoping, who initiated a phase of opening and reform in China.

After the era of the Cultural Revolution, with the arrival of Deng Xiaoping, China adopted a stance of openness to the world, prioritising its economic development through international trade. During this phase, China moderated its information warfare activities, limiting them mainly to domestic information management to ensure regime stability, without being overly ambitious in the international arena. However, this period also saw the birth of the first doctrinal conceptualisations of information warfare in China. Dr. Shen Weiguang, in 1985, is recognised as the father of the concept in China and defined this phenomenon as "both side's attempt to gain the initiative of the battle through their control over information and flow of intelligence" (Weiguang, 1985).

The 1991 Gulf War conflict was to be a turning point for China. Noting US supremacy in the information domain and its ability to use precision weapons and intelligence against the adversary, China recognised the need to invest and adapt. This post-Gulf War period also saw technology and digitalisation begin to play a more prominent role in China´s strategy, inspired in part by US developments (Cheng, 2011).

During the 1990s, military figures such as General Wang Pufeng (Pufeng, 1995) and Colonels Wang Baocun and Li Fei enriched and expanded China´s conceptualisation of information warfare (Neilson, 1997). Wang Pufeng linked it to network warfare, highlighting the relevance of information technology, while Wang Baocun and Li Fei took a more technological approach, relating information warfare to network technology and sensorisation on the battlefield.

Liang Zhenxing and General Yan Banggen, for their part, proposed a broader and more holistic definition that encompasses not only the military aspect, but also the wider struggle for supremacy in the acquisition, control and use of information in all spheres of society (Zhenxing, 1997). In doing so, it revolutionised its understanding and application of information warfare from its historical roots to the most modern conceptions, integrating it into its foreign policy, both civilian and military.

In this sense, China´s Three Wars doctrine (三战), set out in the Political Work Regulations of the People›s Liberation Army in 2003 (PCCh, 2003), is a clear manifestation of how the Chinese Communist Party and the People›s Liberation Army (PLA) continued to conceptualise and adapt their approaches to warfare in the information age. In this context, the three wars refer to:

– **Psychological warfare** (心理战)

  It aims to influence and undermine the morale of the opponent, be it the general population, the leadership structure, or the armed forces. It seeks to establish or promote narratives that favour China´s position, while undermining opposing positions and perspectives.

– **Media wars** (舆论战)

  This war focuses on the battle of narratives in the public information space, especially through media. Its aim is to dominate the discourse and ensure that the Chinese perspective is dominant or, at least, widely represented and accepted.

– **Legal warfare** (法律战)

  Also known as lawfare, this strategy involves the use of international and national laws to achieve strategic objectives. China has used legal arguments, for example, to justify its territorial claims in the South China Sea.

These three wars demonstrate how China has conceptualised conflict in the information space, moving beyond the realm of conventional warfare and into the cognitive realm, harnessing all mechanisms in the information space to its advantage. This approach has progressively increased following Xi Jinping›s rise to power, and China´s foreign policy shift towards a more assertive stance in international affairs.

In terms of its application today, China´s information warfare doctrine, while not solely reflected in a series of official documents, emanates from the various historical publications by its intellectual elite, as well as from the General Doctrine of the Armed Forces and defence white papers. It emphasises the pursuit of the total

computerisation of its armed forces, the development of technology and cyberforces, as well as the application of the Three Wars framework within an all-out war scenario, which Colonels Liang and XIangsui defined in their doctrinal vision as unrestricted warfare (Chew, 2018).

Thus, China´s information warfare doctrine has evolved, incorporating a mix of elements borrowed from the US doctrine, as well as its Soviet heritage with its own historical elements such as the concept of people›s war, targeting weak points, deception and false flag attacks (Charon, 2021).

From the 2015 edition of China´s Defence White Paper (China, gov.cn, 2015) we can see how the People›s Liberation Army (PLA) has devoted and is devoting significant resources to the computerisation of its forces. This process is not limited to guaranteeing access to military intelligence and deception operations to the PLA but encompasses the control of information inputs and outputs across all military elements as a critical component of national security. This approach was confirmed and expanded in the 2019 edition of the same publication entitled China´s National Defence in the New Era (China, gov.cn). The document expanded the information domain by identifying three global spaces of particular security concern, namely outer space, nuclear and cyberspace. Including cyberspace as a domain of special interest, as well as outer space which is especially dependent on information management, China consolidated its doctrinal approach linked to the computerisation of warfare.

In the PLA›s cyber domain, cyber warfare is vital to information warfare, focusing on accessing and occasionally damaging enemy systems. These operations aim to strengthen the country›s power, complement intelligence gathering, map foreign networks and improve defensive capabilities. In turn, China maintains psychological warfare, employing propaganda in information warfare to influence public opinion abroad. To this end, it employs local activists linked to the government to modulate opinion on social networks and in Asian media. These patriotic activists, aligned with the country›s people›s war, can be employed to alter public opinion online. In turn, the control of internal discourse protects its information rearguard.

For practical purposes, this doctrinal consolidation materialised in the establishment in 2015 of the PLA Strategic Support Force (SSF), centralising space, cyber, electronic warfare and psychological warfare missions under a single organisation, progressively absorbing the capabilities of the third and fourth departments of the PLA (Costello, 2018). The launch of the SSF was a particularly significant event in that it materialised the CCP authorities› realisation of the enormous strategic value of the information domain and especially its cross-cutting nature as an enhancer or even enabler of comprehensive operations in the rest of the conventional domains. Similarly, the SSF would also serve as a capability development centre enabling the PLA to professionalise in the various sub-domains in information warfare.

Along with the restructuring of the armed forces, the CCP began to adapt its legal architecture to modern information warfare. On July 1, 2015, the National Security Law of the People›s Republic of China was passed (China, ilo.org, 2015) covering a

multitude of areas related to state security, designed to manage both internal and external security threats in China. The law, which is currently in force, is made up of 84 articles distributed in ten chapters that deal with various aspects such as political, territorial, military, economic, cultural, social and technological security. With regard to technology, the law is notable for its special attention to the domain of cyberspace. It broadly underlines the centrality of the CCP›s leadership and the need to safeguard political stability in the country, allowing for a crackdown on political dissent under the justification of the concept of political security.

The cyber approach emphasises the country›s cyber sovereignty, promoting internet control, censorship and surveillance. article 11 states that everyone in China must cooperate in the security of the state in accordance with the law. Although ambiguous, it suggests that they must assist the state if information or assistance related to national security is requested, or they could be charged with treason. The 2017 Cyber Security Law requires ICT companies to cooperate with government investigations and store Chinese user data within the country.

The next and final step in the materialisation of China´s information warfare capabilities is the splitting of the SSF into three new dedicated agencies, further emphasising the importance of the information domain.

The three new agencies, placed directly under the direct supervision of the CCP›s Central Military Commission, include the Information Support Force (direct heir to the SSF) complemented by the Cyberspace Force and the Military Space Force. Each of these new entities absorbs one of the specific dimensions of information warfare, all of which are directly coordinated by the country›s highest military authority, Xi Jinping (Singer, 2024).

China´s current approach to information warfare is thus articulated through two main avenues, namely the total computerisation of military systems and technical warfare in this domain, and the use of media and communication systems to conduct global influence campaigns. To execute this strategy, the Chinese Communist Party puts all the mechanisms of the state at its service in a systemic people›s war approach.

### *3.4. Comparative analysis*

Information warfare is a cross-cutting phenomenon, involving all states as well as a significant number of non-state actors. The great powers, because of their stance and their constantly conflicting interests, apply this framework of conflict to gain strategic advantages without resorting to arms. At present, the US, the People›s Republic of China and Russia are the main actors in the conflict, due to their technological and social development, their military-political tradition and their global interests.

In this regard, the United States stands out for its sophisticated and structured defence doctrine, which naturally carries over into the realm of information warfare. Thus, the establishment of a clear doctrine and its open dissemination is, to a large

extent, a result of its democratic system, which promotes open and transparent communication on foreign and defence policy. In military terms, its doctrine is detailed in the *Joint Publications*, of the Department of Defence, while, in broad terms, the country›s strategic intentions and movements are set out in National Security Council documents.

In its modern approach to warfare, the United States has adopted a strategy based on multidomain integration, gradually positioning information as the central core of the battlefield. From a cognitive perspective, there has been a remarkable shift in the US approach: the nation has evolved towards STRATCOM, leaving behind traditional psychological operations, which are now handled in secret by its intelligence services.

US global influence extends beyond military force. Thanks to its dominant audiovisual and cultural industry, and its centrality in the Western media, the United States exerts a powerful influence —or soft power— over the West and much of the world. This position is reinforced by educational and support programmes, allowing the US to avoid direct conflict in the digital realm, reserving such tactics for very specific situations.

Additionally, in response to challenges posed by other great powers in the disinformation arena, the United States has invested heavily in media literacy initiatives and anti-disinformation campaigns. Organisations such as USAGM and the recently established FMIC agency, which operates under the Office of the Director of National Intelligence, are clear examples of these efforts. The United States is similarly renowned for its remarkable sophistication and precision in military and intelligence operations. This prowess is a direct product of its robust military-industrial complex, a feature that differs drastically from the approach taken by Russia. US meticulousness and efficiency in the military realm has been evidenced in high-calibre strategic operations such as Olympic Games (Kamiński, 2020) targeting Iran›s nuclear programme, and the more recent Operation Triangulation (Kucheryn, 2023) which targeted the selective interception of communications on Russian territory.

However, despite its leadership in the information domain, the United States faces considerable vulnerabilities in this landscape of conflict. One of the main weaknesses lies in the country›s extensive and tangled network of intelligence and military services. This densely bureaucratised infrastructure is often slow, presenting challenges in terms of effective communication and coordination. At the same time, the US democratic system›s strong commitment to individual freedom and its natural resistance to censorship, while virtuous, can act as a double-edged sword. Respect for these principles can complicate rapid decision-making and, in certain circumstances, give an advantage to adversaries operating with fewer constraints.

Unlike the United States, Russia does not have a comprehensive and structured doctrinal framework for information warfare; public information on the subject is scarce. Thus, on the basis of scant official documentation, limited mainly to government-issued national security perspectives, Russia›s national security strategy can be discerned through its concrete actions on the international stage. In this

sense, Russia adopts a guerrilla approach to information warfare. Despite lacking the technical sophistication of other powers and facing international isolation, it compensates for these weaknesses with a cost-effective and extremely agile strategy. This approach has its roots in the Soviet era, characterised by techniques of infiltration and manipulation of the political systems of target nations, now adapted to the (new) digital environment.

Russia›s tumultuous transition to the information society after the collapse of the USSR profoundly influenced its approach to information warfare. While the Kremlin and the oligarchs maintain an iron grip on traditional media, the deregulation of the internet has allowed the emergence of a distinctive hacker culture. This culture, which includes active and politicised bloggers and users, eventually evolved into figures such as patriotic hackers and professional trolls.

Since the advent of the new millennium, Russia has strengthened both its capabilities in cyberwarfare and cyberespionage and in the manipulation of the cognitive domain. Its ability to integrate operations in both domains is evident, as seen in the cyber-attacks on Estonia, the attacks on the Democratic National Committee in the US and the constant incursions into Ukraine›s critical infrastructure, all accompanied by disinformation and propaganda campaigns.

Russia›s agility in these operations stems from an approach that gives the different intelligence agencies a great deal of autonomy, to the point of competing each other. In addition, the frequent use of non-state actors, such as the Wagner group, allows Russia to deploy rapid, cost-effective and scalable operations globally, although this brings its own challenges and associated problems.

China has rapidly established itself as an emerging power, positioning itself near the forefront of information warfare. From the late 1990s onwards, Chinese military intellectual elites began to develop their own doctrine in this area, largely influenced by the events of the Gulf War. This development led China to realise the crucial importance of information dominance. Unlike other nations, China does not distinguish between the cyber and psychological aspects of Information Warfare. In its vision, information is a strategic domain in its own right.

Chinese information warfare doctrine has itself undergone a significant metamorphosis over the years. Initially influenced by the Soviet heritage, which prioritised propaganda and the instrumentalisation of communist ideology, China has adapted its approach to a more comprehensive information warfare. This adaptation is based on a combination of technology, psychological operations and international media manipulation. It is noteworthy that, in its evolution, China took inspiration from US doctrine but adapted it according to its Soviet context and legacy.

Today, China is striving for full integration of information in the context of warfare. In its view, all war is, in essence, an information war. This concept is the cornerstone of the Chinese armed forces› modernisation process. Moreover, China´s information warfare has a cross-cutting approach, involving all actors in society. In keeping with the country›s communist heritage, the people›s war remains a central strategy, with

the Communist Party having the ultimate responsibility for managing and directing these operations.

At a strategic level, the People›s Republic of China has incorporated information warfare into its Three War doctrine: media, legal and psychological. Through these, it seeks to exert political, diplomatic and communicative pressure, gradually escalating and using all available resources in the information space. The overriding objective is to build an international arena that is conducive to China´s foreign policy. This is achieved through media manipulation, the reinterpretation of international law to its advantage, and aggressive manipulative tactics ranging from military intimidation (as in the case of Taiwan) to disinformation campaigns and online harassment, exemplified by tactics such as wolf warrior diplomacy.

Internally, the Chinese state has instituted strict control over the flow of information. This control is materialised through various mechanisms: constant propaganda aimed at the population, advanced technological surveillance systems such as the Golden Shield and, of course, the omnipresence of the Communist Party which monitors and guides all aspects of society. In fact, China´s information warfare is not just a strategy of the upper echelons of government; it is an approach that is woven throughout society, involving both individuals and corporate entities.

In this context, strategic Chinese companies, ranging from large telecommunications operators to social media giants, play a crucial role. Under national security law, these companies can be mobilised to contribute to the country›s information warfare efforts. This integration of companies into national information strategies is significantly more systematic and structured than in countries such as Russia. Moreover, China´s position as a global technological and economic power gives it a sophistication that surpasses the Russian approach and presents an agility that, in many respects, challenges even the United States.

From a military perspective, this information warfare doctrine has led to significant reorganisations within the PLA. A relevant milestone in this process was the creation of the Strategic Support Force in 2015 as an integration and development force for the various information warfare capabilities in the country, and its subsequent expansion into three specific agencies in the communication, cyber and space sub-domains under the direct command of the Central Military Commission in 2024.

## 4. Conclusions

Since the dawn of civilisation, organised groups of all kinds have sought supremacy in the information domain, to secure or support their control over physical territory. However, the real transformation in this struggle over the years has come about through technological and social advances, which have redefined the strategies, tactics, techniques and procedures of the actors involved. The consolidation of information warfare as a relevant mode of combat took hold in the 20th century, especially with

the rise of ICTs in the new millennium. This contemporary approach divides into two domains: the cognitive, in which propaganda, deception and disinformation are the main weapons; and the technological, dominated by cyberwarfare, electronic warfare and cyberespionage.

To understand the complexities of today›s information warfare, it is essential to analyse it through the prism of the operations of the three great powers: The US, Russia and China. Each of these powers approaches information warfare with its own unique approach, but regardless of how they act, they all share a common goal: to consolidate and expand their influence in the international system. Offensive realism offers a clear perspective for understanding this phenomenon. At their core, the great powers, in their quest for hegemony, are destined for clash and conflict. This clash does not only manifest itself in conventional military confrontations, but also in the information arena. Information warfare, because of its low political cost and easy scalability, has become an essential, indispensable tool for these powers. The struggle for political and cultural influence over the international system results in a constant battle in the information domain.

Thus, in this new global scenario, information warfare is not just a possibility, it is an inevitable phenomenon. The great powers, through their vast resources and capabilities, are engaged in a constant struggle to define and redefine reality, influence perceptions and control the flow of information in an increasingly connected world. The information domain has undoubtedly become one of the main arenas of conflict in contemporary international politics. The doctrinal study of information warfare through the great powers allows for an in-depth understanding of the phenomenon. Given their capacity for innovation and leadership in large-scale operations, these nations not only set standards, but also influence the direction and position taken by other powers in this field, often generating alliances and common fronts.

Despite sharing certain similarities, especially in their growing interest in competition in this domain since the Second World War, the techno-political realities of these powers have led them down different paths. China and Russia, under the ideological umbrella of communism, have adopted information warfare with a focus on political influence. In particular, Russia, strengthened by Cold War tensions, invested heavily in sabotage and information manipulation, which has characterised its aggressive approach, now adapted to the digital realm.

On the other hand, the US has adapted its strategy of defending democracy using advanced technology, cyber weapons and cyberspace operations to support its international position. China in turn, combining experiences from the US and its Soviet heritage, has created an information-centric strategy, merging civilian and military efforts under the Communist Party.

This current panorama suggests an intensification of Information Warfare in the years to come. The powers will advance their doctrines, seeking greater sophistication and integration. While conventional military power still dominates the dynamics of international conflict, modern warfare increasingly tends towards information

warfare. The objective will be to destabilise and disrupt enemy command and control capabilities at all levels, from influencing public perception to disrupting vital telecommunications systems. Ultimately, whether on the plains of Eastern Europe, on the island of Formosa or even within Western democracies, information will be the key to power. Its control and manipulation will decide the outcome of confrontations, both in the international political and military arenas.

As we have discussed in this paper, information warfare is a phenomenon that is as permanent as it is inevitable. Because of their global interests, as well as the breadth and social complexity of their territories, the great powers are forced to interfere in the information domain, whether to coordinate the collective action of their vast human resources, to facilitate cooperation with distant populations or to obtain strategic information. Information warfare between such powers is inevitable, as we have seen in the cases of Russia and China, precisely as a country achieves (or regains) great power status it is naturally forced to compete in that domain, whether by fighting for narrative or by expanding and sophisticating its intelligence and sabotage capabilities.

The recognition and study of this mode of warfare is therefore more than imperative for leaders and strategists, both in these countries and especially in middle-ranking and lesser powers, among which, for example, we find Spain. These powers, because of their lesser capacity for influence, often limited to their immediate geographical surroundings, are strongly influenced by both doctrinal developments and the actions of the great powers. Having less weight in the international system, depending on political, economic and military alliances dominated by the great powers, these states become battlegrounds where the great powers struggle for influence. As a result, they are often victims of digital or conventional espionage campaigns, influence peddling, interference and political manoeuvring of all kinds. This can already be observed today in Latin American regions, and to a lesser extent in Western Europe. Even traditionally influential powers like Israel, capable of defending themselves technically and narratively, are often implicated in the power dynamics of great powers through the information domain.

Against this backdrop, it is imperative that these powers develop their own information warfare capabilities, especially those with systems based on liberal democracy, which are much more vulnerable to destabilising action from powers with autocratic regimes. It is therefore essential to legally reinforce these capabilities through laws regulating the activity of foreign agents, be they intelligence services or political groups linked to foreign powers. The primacy of foreign agent laws such as the one in the US over the recently discussed anti-disinformation laws puts the focus on foreign interference beyond content, guaranteeing state protection as well as the right to freedom of expression in the face of political censorship. Similarly, it is essential to increase counterintelligence and cyber intelligence capabilities, both at the human and technological levels, while fostering greater communication and transparency towards society in order to reinforce confidence in these organisations, as has already been pointed out by Maddox *et al.* (2021). Militarily, the cross-cutting nature of the phenomenon must be recognised and robust communication

mechanisms in the chain of command and, in particular, specialised units capable of handling the full cycle of information warfare must be established, integrating both technical and communication capabilities. In terms of training, military academies and think tanks should be able to train new generations of military cadres in specific information warfare profiles, from psychology to cybersecurity. The implementation of such measures will ensure a more efficient defence adapted to the contemporary challenges of the global geopolitical environment.

## Bibliography

Affairs. (2023). Chinese Definitions of Information Warfare. *Global affairs.* [Accessed: 2024]. Available at: https://www.globalaffairs.ch/2022/06/08/chinese-definitions-of-information-warfare/Aro, J. (2016). The cyberspace war: propaganda and trolling as warfare tools. *European view*. 15, 1, pp. 121-132.

Ateş, A. (2020). The Transformation of Russian Intelligence Community After the Cold War (1991-1993). *Karadeniz Araştırmaları*. 66, pp. 321-332.

Azad, T. M. (2023). Understanding Gray zone warfare from multiple perspectives. *World Affairs*. 186,1.

Bates, S. (2010). Disinforming the world: Operation INFEKTION. *The Wilson Quarterly*. 34, 2.

Bittman, L. (1985). *The KGB and Soviet disinformation: an insider›s view*. Pergamon.

Военная доктрина Российской Федерации [online]. (2010). *Kremlin.ru*. [Accessed: 2024]. Available at: http://www.kremlin.ru/supplement/461

Brantly, A. F. (2020). A brief history of fake: Surveying Russian disinformation from the Russian Empire through the Cold War and to the present. En: Whyte, C. *Information warfare in the age of cyber conflict.*

Bruzesse, M. y Singer, P. (2024). Farewell to China's Strategic Support Force. Let's meet its replacements [online]. *Defense One*. [Accessed: 2024].

Charon, P. and Jeangène VIlmer, J. B. (2021). *Chinese influence operations, A Machiavellian moment*. París, Institut de Recherche Stratégique de l›Ecole Militaire.

Cheng, D. (2011). Chinese lessons from the Gulf Wars. En: Scobell, A., Lai, D. y Kamphausen, R. *Chinese lessons from other peoples' wars*. ISBN: 1-58487-511-9

Chew, J. (2018). *How China Applies its «Principles of Unrestricted Warfare» in the 21st Century*. Raportti, Galisteo Consulting Group. Haettu, 30.

China's Comunist Party. (2003). The Circular of the CCP Central Committee on Chinese People's Liberation Army Political Work Regulations (中共中央关于

颁布《中国人民解放军政治工作条例》的通知). *News of the Communist Party of China.*

China, T. S. (s. f.). China´s National Defense in the New Era [online]. *gov.cn.* [Accessed: 2024]. Available at: http://eng.mod.gov.cn/xb/Publications/WhitePapers/4846452.html#:~:text=This%20is%20the%20strategic%20guidance,response%2C%20and%20adopts%20active%20defense

—. (2015a). China's Military Strategy [online]. *The State Council The People's Republico f China*. [Accessed: 2024]. Available at: https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm

—. (2015b). National Security Law of the People›s Republic of China [online]. *ilo.org*. [Accessed: 2024]. Available at: https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=111289&p_lang=en

Concepto de la política exterior de la Federación de Rusia [online]. (2023). Министерство иностранных дел Российской Федерации. *kremlin.ru*. [Accessed: 2024].

Costello, J. A. (2018). China´s strategic support force: A force for a new era. Testimony to the U.S.-China Economic and Security Review Commission. *Ministry of National Defense of the People's Republic of China.*

Darczewska, J. (2014). The anatomy of Russian information warfare. The Crimean operation, a case study. *OSW*.

—. (2015). The devil is in the details. Information warfare in the light of Russia›s military doctrine. *OSW*.

Duguin, A. (1999). *Proyecto Eurasia Teoría y Praxis*. Hipérbola Janús.

Evan, M. K. (2022). Moscow›s Strategic Culture: Russian Militarism in an Era of Great Power Competition. *Journal of Advanced Military Studies*. 13,1.

Fabian, S. (2019). The Russian hybrid warfare strategy-neither Russian nor strategy. *Defense & Security Analysis*. 35,3.

Fei, W. B. (1997). Information Warfare. In: Pillsbury, M. *Chinese Views of Future Warfare*. Washington D. C., National Defense University Press.

Galán, C. (2023). El ecosistema de propaganda rusa. *Política exterior.*

Galeotti, M. (2016). Putin›s hydra: inside Russia›s intelligence services. *European Council on Foreign Relations*.

Gerasimov, V. (2016). Hybrid Warfare Requires High-Tech Weapons and a Scientific Basis. *Military-Industrial Courier*.

Gilpin, R. G. (1984). The richness of the tradition of political realism. *International organization*. 38, n.º 2, pp. 287-304.

Green, K. R. (2016). People›s War in Cyberspace: Using China´s Civilian Economy in the Information Domain. *Military Cyber Affairs*.

Guerasimov, V. (2013). The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*.

Harknett, R. J. (1996). Information warfare and deterrence. *The US Army War College Quarterly*. 26, 3, pp. 93-107.

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington, Virginia, Potomac Institute for Policy Studies.

Jincheng, W. (1996). Information war: a new form of people›s war. *Liberation Army Daily*.

Johnson, L. S. (2004). A Major Intelligence Challenge: Toward a Functional Model of Information Warfare. *CIA: Lessons in Intelligence*. 392.

Kamiński, M. A. (2020). Operation «Olympic Games». Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme [online]. *Security and Defence Quarterly*. 29. [Accessed: 2024]. DOI: https://doi.org/10.35467/sdq/121974

Keating, K. C. (1981). Maskirovka: The Soviet system of camouflage. *US Army Russian Institute*.

Kucheryn, G. (2023). The outstanding stealth of Operation Triangulation [online]. *Securelist*. [Accessed: 2024]. Available at: https://securelist.com/triangulation-validators-modules/110847/

Laswell, H. D. (1948). The structure and function of communication in society. *The Communication of Ideas*.

Liang, Q. A. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House Arts.

Libicki, M. C. (1995). *What is information warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University.

—. (2017). The convergence of information warfare. *Strategic Studies Quarterly*. 11.1.

Lippman, W. (1946). *Public opinion*. New York, Penguin Books.

Liu, M. (2024). The «Gray Zone» Conflicts in China-US Relations: From a Geopolitical Perspective. *International Journal of Education and Humanities*.12, n.º 1.

Lysenko, V. A. (2018). Russian information troops, disinformation, and democracy. *First Monday*. 23, n.º 5

Maddox, J. D. (2021). Toward a Whole-of-Society Framework for Countering Disinformation. In: *Great Power Cyber Competition*. London, Routledge.

Mally, L. (2003). Exporting Soviet culture: The case of Agitprop theater. *Slavic Review*. 62, n.º 2.

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. Nueva York, WW Norton & Company.

—. (2021). The inevitable rivalry: America, China, and the tragedy of great-power politics. *Foreign Affairs*.

MEMBERS OF THE IC [online]. (2023). *ODNI*. [Accessed: 2024]. Available at: https://www.dni.gov/index.php/what-we-do/members-of-the-ic#:~:text=The%20CIA%20is%20separated%20into,and%20Offices%20of%20the%20Director.

Miles, R. (2021). Russia in Latin America. In: *External Powers in Latin America*.

Mittler, B. (2014). *A Continuous Revolution: making sense of Cultural Revolution culture*. Harvard University Asia Center Publications Program.

*National Intelligence Strategy* [online]. (2023). *ODNI*. [Accessed: 2024]. Available at: https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

Ota, F. (2014). Sun Tzu in contemporary Chinese strategy. *Joint Forces Quarterly*. 73, n.º 2.

Neilson, E. (1997). *Sun Tzu and Information Warfare*. National Defense University.

Nye, J. S. (1990). Soft power. *Foreign Policy*. N.º 80.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare.*

Perez, E. V. (2023). El giro Indo-Pacífico de la política exterior de Estados Unidos: una aproximación geopolítica desde el realismo neoclásico. *Revista Del Instituto Español De Estudios Estratégicos*. 20.

Pillsbury, M. (1998). *Chinese views of future warfare*. National Defense University.

President of Russia. (2014). The President approved new edition of Military Doctrine [online]. *Kremlin.ru.* [Accessed: 2024]. Available at: http://www.en.kremlin.ru/events/president/news/47334

Pufeng, W. (1995). The Challenge Of Information Warfare. *China Military Science*.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*. 22, n.º 3, pp. 283-300.

Robinson, M. K. (2015). Cyber warfare: Issues and challenges. *Computers & Security*. 49, pp. 70-94

Robinson, P. (1999). The CNN effect: can the news media drive foreign policy? *Review of International Studies*. 25, n.º 2, pp. 301-309.

Ruiz, M. G. (2018). La viñeta, la nueva Arma durante la I Guerra Mundial. *Revista Del Instituto Español De Estudios Estratégicos (IEEE)*. 9.

Rumer, E. (2019). The Primakov (not Gerasimov) doctrine in action. *Carnegie Endowment for International Peace*.

Sampanis, S. E. (2024). Cyberwarfare in the Modern World. Hybrid Threats, Cyberterrorism and Cyberwarfare. *CRC Press*.

Sanger, D. E. (2016). Spy agency consensus grows that Russia hacked DNC. *New York Times*.

Soriano, M. T. (2018). Guerras por Delegación en el Ciberespacio. *Revista Del Instituto Español De Estudios Estratégicos (IEEE)*. 9, pp. 15-36.

Staun, J. A. (2023). Russian influence operations in the wars in Ukraine in 2014 and 2022: active measures and maskirovka. *Politica*. 55, n.º 2.

The White House. (2022). *National Security Strategy* [online]. [Accessed: 2024]. Available at: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

USA-JCS. (2022). *Joint Publications Operations Series*. *jcs.mil* [online]. [Accessed: 2024]. Available at: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

Votel, J. L. (2016). Unconventional warfare in the gray zone. *Joint Forces Quarterly*. 80, n.º 1.

Waltz, K. (2018). *Man, the state, and war: A theoretical analysis*. Columbia University Press.

Weiguang, S. (1985). *Information warfare*.

Woolley, S. C. (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford, Oxford University Press.

Zhenxing, L. (1997). New military revolution and information warfare. Zhongguo dianzi bao.

рф. (2013). Концепция внешней политики Российской Федерации [online]. *kremlin.ru.* [Accessed: 2024]. Available at: http://static.kremlin.ru/media/events/files/41d447a0ce9f5a96bdc3.pdf

рф. (2015-2021).. Национальная стратегия безопасности [online]. *kremlin.ru*. [Accessed: 2024]. Available at: http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf

рф. (2016). Доктрина информационной безопасности Российской Федерации [online]. [Accessed: 2024]. Available at: https://d-russia.ru/wp-content/uploads/2016/06/doktrina_informacionnoi_bezopasnosti_rf.pdf

РФ, П. (2014). Военная доктрина российской федерации [online]. [Accessed: 2024]. Available at: http://emsu.ru/extra/pdf5s/lobbyist/2014/6/24.pdf

Панарин, И. (2021). пропаганда и информационные войны.

*Article received: October 28, 2023.*
*Article accepted: May 19, 2024.*