**The Ideological Roots of National Cyber Doctrines: Comparing Russia and China’s Cyber Operations in Outer Space**

Louise Demiral, Department of Political Studies, Bar-Ilan University

Elai Rettig, Department of Political Studies, Bar-Ilan University

**Abstract**

This study explores the divergent cyber strategies of Russia and China in outer space. Although both share advanced satellite infrastructure and recognize the United States as a common rival, they differ markedly in doctrine and ideology. Russia’s approach is largely offensive, combining disruptive cyber-attacks on satellites and navigation systems with extensive information warfare. China, in contrast, pursues a preventive and defensive strategy of denying adversaries similar capabilities through espionage and signal jamming, viewing cyberspace as a realm of vulnerability that must be monitored and controlled to guard its economic progress, social stability, and national security. This study argues that these different orientations stem more from political-ideological factors than from disparities in technical or economic capacity. By examining Russia’s use of cyber-attacks during its invasions of Ukraine and China’s jamming activities in the South China Sea, the study illustrates how cultural and historical conceptions of “information warfare” drive each superpower’s policies in space. The analysis concludes by pointing to a growing security dilemma in the largely unregulated domain of outer space, where cyber operations risk widespread disruptions. In calling for heightened international awareness, the study underscores the magnitude of potentially destabilizing space-cyber activities for states, societies, and global security.

1. **Introduction**

Space has re-emerged as a theater of intense strategic rivalry in the twenty-first century, with Russia and China both seeking to modernize their militaries and challenge Western primacy (Reesman & Wilson 2020). After an era of cooperative initiatives such as the International Space Station and commercialization trends in launch services, recent years have witnessed renewed militarization and the rise of “counterspace” capabilities that aim to negate or disrupt an adversary’s orbital assets (Weeden & Samson 2019). For states like Russia and China, membership in this “space club” conveys great-power standing, advanced technological know-how, and a platform to assert global influence (Paikowsky 2017). Yet because satellites are heavily reliant on cyberspace for data and command signals, they can be sabotaged by actors with relatively modest investments in hacking tools. The low cost and plausible deniability of such methods, coupled with incomplete regulatory oversight, make space-cyber operations particularly attractive for states seeking power projection without overt escalation (Falcão Serra 2021; Meyer 2016; Sadeh 2010).

Within this contested environment, satellites have become indispensable for both civilian and military applications. Civilian societies depend on them for communication networks, navigation, resource monitoring, and more, while military planners rely on orbital infrastructure for intelligence gathering, surveillance, and precision strikes (Reesman & Wilson 2020; Weeden & Samson 2019). Such critical reliance on space assets creates unique security dilemmas (Pavur and Martinovic 2019). Targeting a satellite’s ground station or manipulating its software can impose outsized costs on an adversary, whether by degrading battlefield awareness or hampering vital economic functions. This emerging blend of space and cyberspace has already prompted numerous scholarly discussions on how states incorporate orbital cyber capabilities into broader strategies, or how national doctrines of “information warfare” shape offensive and defensive postures (Li 2023; Febbraro 2023; Martin 2023; Racionero-Garcia and Shaikh 2024). However much of the current research focuses on Western powers, leaving Russian and Chinese practices comparatively understudied.

Although Russia and China both share advanced cyber expertise, both treat the digital domain as part of their national security doctrine, and both hold a recognized rivalry with the West, they follow divergent doctrinal paths for how they use their cyber capabilities in space. Russia is widely believed to have used overtly offensive cyber operations against satellites and satellite communications in conjunction with conventional military invasions, as in Ukraine in 2014 and again in 2022. By contrast, China’s approach has thus far been described as more preventive or “defensive,” implementing jamming measures and anti-access/area denial strategies around the South China Sea while generally avoiding conspicuous or highly destructive attacks on rivals’ orbital assets. The distinguishing factor, this study contends, lies less in raw technical capacity than in the deeper political-ideological traditions each superpower brings to the domain of space security.

The purpose of this article is to illuminate the core factors that lead Russia toward offensive cyber strategies in space, while China tends to prefer a preventive or defensive model. In both states, information warfare is integral to national doctrine, yet each imbues the concept with distinct ideological content. Russia has long embraced active measures and reflexive control, aiming to manipulate or destabilize foreign environments through disinformation and sabotage. China’s emphasis on the “three warfares” (public opinion, psychological, and legal) is typically positioned to secure China’s broader economic and political interests by preventing foreign intrusion, rather than conducting large-scale destabilization in external theaters.

To test whether these broad strategic distinctions indeed apply in the space domain, the article compares Russia’s cyberspace activities in the war on Ukraine (2014–2022) with China’s jamming and spoofing in the South China Sea (2012–present). The comparison suggests that differences in political and ideological objectives, particularly the desire to sow chaos or deter challengers, ultimately shape how each superpower deploys cyber means in space. It also raises questions about how each superpower will approach future escalations as outer space becomes a more hotly contested frontier.

1. **Literature Review**
   1. ***The Significance of the Space Domain in National Security***

The space domain has grown indispensable for modern societies in both civilian and military capacities. Civilian enterprises rely on satellites for telecommunications, navigation, crop monitoring, weather forecasting, and countless other applications that have become routine elements of daily life (Paikowsky 2017). Military planners rely heavily on satellites for intelligence, surveillance, reconnaissance, communication, and geolocation. As a result, outer space has become a new frontier of inter-state competition, especially in regard to cyber vulnerabilities inherent in the orbital infrastructure (Shahzad, Qiao & Joiner 2022). Because satellites depend on ground stations, radio uplinks, data routing, and software-defined networks, they offer a growing “attack surface” for malicious intrusion (Manulis et al. 2020).

The intensifying reliance on satellites is both an opportunity and a risk. Through robust satellite constellations, states can enjoy improved situational awareness, superior command and control of their forces, and heightened capacity to detect and react to strategic threats. However, these same satellites can be jammed, spoofed, or subjected to destructive cyber-attacks (Falco 2018). As space systems incorporate more advanced, software-defined radios, cloud data processing, and integrated sensor networks, their vulnerability to malicious access increases in tandem. Researchers emphasize that potential adversaries may not even need to launch a kinetic anti-satellite (ASAT) projectile. Instead, an intrusion into ground stations or satellite software can disrupt critical functionality without physically destroying the asset (Weeden & Samson 2019). This feature underscores the continuum between purely “cyber” operations and what might be viewed as “electronic warfare,” further blurring conventional lines between warfighting domains.

The rapid expansion of space technology during the twentieth and twenty-first centuries has also reshaped military, economic, and social life around the world. In addition to its application to surveillance, communications, and geolocation, the space domain has gradually intertwined with cyberspace, forming a complex interplay of orbital infrastructure, digital systems, and global networks (Paikowsky 2017). Early space activities, such as reconnaissance satellite systems during the Cold War, paved the way for the more integrated uses we witness today, ranging from satellite-based navigation and communications to the global positioning systems that guide civilian and military platforms. As the capabilities of these systems expand, so do their vulnerabilities to cyber-attacks (Shahzad, Qiao & Joiner 2022). What was once the exclusive province of a few advanced powers is now critical for every state that relies on ubiquitous connectivity, trade, and security cooperation.

This evolution has heightened the importance of outer space for national security and economic development, while exposing new and profound weaknesses. The digital infrastructure for satellites, ground stations, signal processing, and data transfer has become a prime target for states seeking to gain asymmetric advantage (Manulis, Bridges, Harrison, Sekar, & Davis 2020). At the same time, satellites are central to national defense and daily civilian life, whether in the form of weather forecasting, resource monitoring, or battlefield surveillance. A concerted cyber-attack on satellite constellations or their associated ground stations can result in large-scale societal disruption, from disabling navigation services to interrupting communications and data access for millions of people (Falco 2018). Part of the reason for this vulnerability is the distributed nature of the space infrastructure, which links satellites, ground facilities, and various networked systems through radio frequencies, remote uplinks, and an array of complex software.

States increasingly incorporate these space-based assets into their national security postures. Four leading global navigation satellite systems, GPS (U.S.), GLONASS (Russia), Galileo (EU), and BeiDou (China), form the backbone of global communications and commerce. These systems, and the satellites that support them, are acknowledged as critical infrastructure with considerable strategic, economic, and social value (The White House 2020). Unsurprisingly, leading powers now regard space as an integral component of modern defense strategy, seeking either to preserve assured access or to deny it to potential adversaries (Reesman & Wilson 2020). The interplay between major powers in space, including the potential deployment of counter-space capabilities, has raised the prospect that future conflict will extend beyond land, sea, and air domains to orbital systems, even reaching the Moon.

Although satellites have traditionally been discussed within the context of rocket engineering and orbital physics, cyberspace has emerged as a critical enabler of modern space operations. The underlying dependence on digital signals and network connectivity allows hackers to compromise satellites’ ground control, falsify their data, or hijack their command functions with relative stealth (Pavur and Martinovic 2019). These vulnerabilities are compounded by incomplete regulatory frameworks that have yet to comprehensively address cybersecurity in space (Falcão Serra 2021; Meyer 2016; Sadeh 2010). As more states integrate satellite services into their defense and commercial sectors, the interconnected nature of cyber and space domains presents novel security threats that extend well beyond the bounds of traditional warfare.

While several scholars have begun to examine how cyberspace shapes the tactics and tools of space-based competition (Li 2023; Febbraro 2023; Martin 2023), much remains unknown about how these capabilities fit into broader national security strategies. Certain key questions persist: to what extent do states perceive cyber operations in orbit as a distinct category of military action, and how do they conceptualize escalation or deterrence in a realm where few precedents exist? The absence of robust historical analogs for satellite hacking heightens uncertainty, and legal experts note that existing space treaties only obliquely address non-kinetic attacks. As a result, doctrinal approaches to cyber in space are evolving rapidly, driven by real-time crises and ad hoc experiments rather than by established treaties or norms.

These gaps in the scholarship reflect the relatively nascent stage of research into orbital cybersecurity. States have conducted anti-satellite (ASAT) missile tests and engaged in various forms of jamming for decades, but only with the acceleration of digital innovation have purely cyber tactics become a credible and potentially devastating alternative (Pavur and Martinovic 2019). Threat actors can now mask intrusions or attribute them to non-state proxies, making enforcement and retaliation more difficult. Scholars thus highlight an urgent need for analytical frameworks that fully integrate cyberspace considerations into space security discussions, including the legal, strategic, and operational dimensions (Falcão Serra 2021; Meyer 2016; Sadeh 2010). As this body of research expands, it will shed new light on the doctrinal debates and strategic cultures that guide how different states, particularly Russia and China, approach cyber conflict in orbit.

* 1. ***Offensive versus Defensive Cyber Strategies in Space***

Scholars have proposed several frameworks to classify states’ cyber strategies in the space domain. One broad distinction is between an offensive approach, which seeks to control information or degrade adversarial functions, and a preventive or defensive approach, which prioritizes shielding national infrastructure and denying adversaries the same advantage (Cohen & Bar-El 2017). While such labels risk oversimplifying complex realities, they highlight an important question about a state’s willingness to use cyberspace proactively to disrupt rivals. Offensive cyber operations in space might target data links, command streams, or navigation signals, with the goal of sowing confusion or physically disabling the satellites or ground stations. Defensive strategies, by contrast, center on encryption, redundancy, secure hardware, and “hardening” the entire command and control chain against intrusion (Shahzad, Qiao & Joiner 2022). In practice, many states combine these measures, but place greater emphasis on one or the other.

In existing scholarship, Russia is widely portrayed as more offensively oriented. Analysts note the historical Soviet tradition of reflexive control and active measures, in which the aims often involve manipulating the adversary’s perception or generating chaos in rival societies (Baram & Bar-El 2019). Examples include the 2007 and 2008 cyber incidents in Estonia and Georgia, as well as repeated disruptions of Ukrainian infrastructure beginning in 2014. Similar logic is evident in Russian attempts to jam signals in war zones and sabotage adversarial communications satellites. Although Russia frames these activities in defensive terms, researchers argue they are more accurately described as opportunistic and aimed at unsettling opponents.

China’s strategy, by contrast, is described by many analysts as “preventive” or “defensive” (Baram & Bar-El 2019; Hoffman 2019). While China’s People’s Liberation Army (PLA) invests heavily in counterspace technology, China often emphasizes denying adversaries the ability to operate overhead while shielding its own assets through robust encryption and electronic warfare defenses. Such an emphasis on defense does not preclude sophisticated espionage or information theft, including infiltration of satellites or ground stations to gather data. Nonetheless, official Chinese discourse and doctrinal writings reference the importance of “three warfares” (public opinion, psychological, legal) in shaping the environment before conflict, so that, ideally, victory is achieved without direct confrontation (Kania 2016). In space and cyberspace, these forms of soft power can be complemented by preemptive measures that degrade an adversary’s satellites if needed but do so in ways that preserve China’s broader priorities of economic development, territorial integrity, and social stability.

Research on the uniqueness of space-cyber operations highlights the distributed architecture of satellite systems and the specialized vulnerabilities in each “segment”: ground stations, user terminals, the space segment, and the communication link (Maini & Agrawal 2014). Attacks can involve deliberate jamming on the ground, spoofing or altering signals in flight, hacking satellite on-board software, or impersonating legitimate commands. While the physics of orbital mechanics differ from those of terrestrial networks, the logic of infiltration, disruption, and denial remains consistent with broader cyber frameworks, save that states can generate strategic or global-scale disruption by targeting the few ground stations controlling entire constellations (Weeden & Samson 2019). As these examples show, scholarship increasingly recognizes that great-power rivalry in space is not solely about launching anti-satellite missiles but about subtle hacking campaigns that degrade or manipulate an enemy’s confidence in its orbital assets.

* 1. ***The Intersection of Ideology and National Cyber Strategies***

Gaps persist in understanding how states incorporate orbital cyber capabilities into broader strategies, or how national doctrines of “information warfare” shape offensive and defensive postures, with current studies predominantly focused on Western powers (Racionero-Garcia and Shaikh 2024). Scholars have made notable progress in analyzing NATO and U.S. cyber force structures, military doctrines, and operational patterns, yet comparatively few studies investigate how non-Western powers, particularly Russia and China, integrate satellite hacking, electronic warfare, and digital espionage into their overarching security frameworks. This oversight is striking when one considers that both Moscow and Beijing have demonstrated sophisticated cyber capacities and publicly emphasized the importance of space assets for their national security. As a result, core questions remain insufficiently answered: How do Russia and China perceive the strategic value of non-kinetic satellite attacks, and in what ways do their domestic ideological or doctrinal commitments inform their willingness to employ these methods?

Addressing these gaps requires a closer look at how each state intertwines concepts of information warfare with its evolving space programs, paying attention not only to technical developments but also to the broader historical and cultural contexts in which these capabilities are embedded. While Western scholarship frequently highlights the integration of cyberspace within NATO’s defense posture, Russia and China articulate visions of space-cyber warfare that are shaped by distinct ideological legacies, security priorities, and institutional practices. By refocusing on these alternative viewpoints, researchers and policymakers can deepen their understanding of the strategic calculus behind satellite targeting, jamming, and digital infiltration, as well as anticipate how such methods might be deployed in future conflicts.

The study of national cyber strategies often focuses on bureaucratic structures, technological development, or doctrinal publications. Equally important, however, are the intellectual and cultural influences that guide each state’s understanding of information warfare. Analysts of Russia’s approach, for example, frequently point to Soviet and Tsarist-era practices of controlling domestic narratives, conducting disinformation abroad, and envisioning war as a political continuum that seamlessly blends overt and covert methods (Wexler & Bar-El 2020). Similarly, scholars of China’s cyber posture cite Confucian ideals of strategic restraint, the concept of war as a last resort, and a preference for shaping the environment before war breaks out (Feng 2005; Kania 2016). Observers note that these longstanding philosophical traditions, combined with the imperatives of the modern Communist Party, generate an emphasis on control of the information domain within state borders, an aversion to chaotic escalation, and a preference for incremental advantage. Precisely how these cultural or ideological threads translate into day-to-day space-cyber tactics remains subject to debate, as official strategic statements sometimes obscure more than they reveal (Gleason 2018; Sharikov 2018).

Methodologically, a comparative study of Russia and China’s strategies in space cyberspace reveals how each superpower reinterprets basic concepts of information and conflict to meet perceived national priorities. While both states conceive of cyberspace as an integral part of national sovereignty, they diverge on whether to prioritize immediate offensive measures. Russia’s repeated willingness to disrupt satellites or degrade adversary connectivity, for instance, may reflect the conviction that sowing chaos in neighboring states preserves Russia’s strategic depth (Martti 2019). By contrast, China’s tradition of focusing on defense and preemption suggests a stronger concern for maintaining stable external conditions so that it can pursue economic modernization and social development (Baram & Bar-El 2019).

Thus, cross-case analysis of Russia’s Ukraine operations and China’s interventions in the South China Sea can help elucidate the motivations behind each power’s distinct path. The next sections examine these divergences in detail.

1. **Research Design**

The objective of this research is to determine why Russia and China, two superpowers with overlapping capabilities, adopt disparate cyber strategies in the space domain. One hypothesis is that these differences cannot be explained solely by technological or economic constraints. Rather, ideological orientations, historical experiences, and distinct interpretations of “information warfare” guide each state’s approach.

This article thus proposes three main hypotheses. First, this study argues that the gap in offensive versus preventive/defensive orientations emerges from underlying ideological and historical traditions. Offensive cyber strategies, as manifested by Russia, treat information warfare as a tool to destabilize foreign targets and expand influence, whereas preventive strategies, as displayed by China, stress the securing of critical national priorities, from territorial sovereignty to economic advancement. Second, it argues that a state that chooses an offensive cyber strategy, like Russia, interprets information warfare as a means of controlling both internal and external information streams. Through hacking, disinformation, sabotage, and reflexive control, Russia uses cyberspace to disrupt adversaries and shape narratives at home and abroad. Though cast as defensive in official documents, such action has a clearly coercive character. Third, it argues that a state that prefers a preventive or defensive cyber strategy, like China, regards cyberspace as a realm of vulnerability that must be monitored and controlled, but primarily to guard economic progress, social stability, and national security. China invests heavily in intelligence gathering, espionage, and the capacity to jam or blind adversarial satellites, but frames these activities in a discourse of denial and deterrence, rather than large-scale chaos creation.

To test these hypotheses, this study employs qualitative comparative analysis of two key cases. The first is Russia’s approach during its conflict with Ukraine from 2014 onward, focusing on how Russia used cyber means in space to augment kinetic operations. The second is China’s use of satellite-based jamming to mask or disrupt signals in the South China Sea from 2012 onward, especially around disputed maritime features. By focusing on these two examples, each of which involves states with advanced cyber tools under different strategic imperatives, we can ascertain whether the variation in approach derives from distinctive historical-ideological frameworks or from more practical concerns. The research draws on government documents, academic studies, news reports, and commercial analyses to reconstruct how each superpower conceptualizes and operationalizes cyber attacks and defenses in space. Although scholars have assessed Russia and China separately, few have juxtaposed their divergent strategies under the same analytical lens of “offensive vs. defensive” orientations in orbit.

This analysis is structured around four parts. First, it reviews the Russian concept of cyber war and information warfare, highlighting major doctrinal statements. Second, it traces how Russia incorporated space-based cyber operations into its invasions of Ukraine. Third, it surveys China’s national cyber doctrine and how it extends to the space domain, especially in the South China Sea. Fourth, the two cases are compared to identify the deeper drivers of divergence, concluding that ideology and national strategic objectives are at least as important as raw material capabilities in shaping each power’s choices.

1. **Case Studies – Russia vs. China’s National Cyber Strategy**
   1. ***Russia’s Cyber Strategy in Outer Space***

Russia’s pursuit of an offensive cyber strategy in the space domain can be understood through a combination of historical traditions, doctrinal developments, and concrete military operations (Giles 2017; 2021; Connell & Vogler 2017). Since the early twentieth century, Russian strategic thought has placed great emphasis on information as a crucial element of warfare (Snegovaya 2020). This thread can be traced back to the Soviet era, where control over domestic and foreign information flows was vital to projecting power both internally and internationally (Bilyana & Cheravitch 2020). In modern Russia, this legacy has evolved into a comprehensive concept of “information confrontation,” blending technical, psychological, and cognitive components. By the beginning of the twenty-first century, Russia refined these approaches to reflect the growing significance of cyberspace and the unique vulnerabilities that now arise in the space domain. Official policy documents, ongoing military reforms, and direct battlefield experience all demonstrate how Russia’s embrace of offensive cyber measures extends well beyond traditional espionage or low-level disruptions to target satellite communications, ground stations, and entire segments of the space infrastructure (Raska 2020).

Early doctrinal shifts around 2000 signaled Russia’s emerging worldview of the internet and global communications networks as extensions of state rivalry. The adoption of the 2000 Information Security Doctrine, and subsequent revisions to military and national security strategies in 2010, 2014, and 2016, repeatedly emphasized external threats to Russia in the “information sphere” (Wexler & Bar-El 2020; Bilyana & Cheravitch 2020). Russian officials contended that an array of Western actors, state agencies, media outlets, technology firms, were exploiting cyberspace to destabilize Russia politically and challenge its sovereignty. In response, Russian authorities enacted robust legislative frameworks designed to regulate domestic digital platforms and to promote “russified” or “sovereign” internet infrastructure. More pertinent to space, however, was the realization that satellites, ground control centers, and satellite-based communications represented both critical national assets and potential vectors for sabotage. Russia resolved to develop a doctrine that treats outer space as an extension of the broader “information battlefield,” thereby justifying the use of disruptive or destructive operations (Bilyana & Cheravitch 2020).

Although official rhetoric consistently frames Russian actions as defensive or countermeasures against a perceived Western threat, many analysts argue that Russia’s activities reflect a decidedly offensive posture (Adamsky 2018; Snegovaya 2020). Researchers note how Russian state-aligned groups conduct long-running cyber campaigns encompassing everything from disinformation to hacking of industrial control systems. Within the space sector, these offensive tendencies become clear in Russia’s repeated GPS jamming in conflict zones, its experimentation with satellite-based internet links to hide hacker locations, and its alleged sabotage of adversary satellite communications (Connell & Vogler 2017). Observers stress that Russia’s approach to the space-cyber nexus is not a separate or entirely novel policy, but rather a seamless extension of Soviet-era reflexive control, repurposed for the interconnected networks of the digital age (Giles 2021). Reflexive control involves manipulating an opponent’s perceptions to gain a strategic advantage, an objective readily pursued through electronic and cyber means in satellite environments (Wexler & Bar-El 2020).

A key factor enabling Russia’s shift toward offensive cyber operations in space is the evolving role of its security services. The Federal Security Service (FSB), successor to parts of the KGB, oversees domestic security but has also become active in cyber espionage and sabotage campaigns outside Russian borders (Bilyana & Cheravitch 2020). The Foreign Intelligence Service (SVR) focuses on intelligence collection abroad, including the infiltration of foreign networks. Meanwhile, the Main Intelligence Directorate (GRU) of the General Staff has proven particularly aggressive in launching large-scale cyber-attacks, as well as combining cyber operations with kinetic military maneuvers (Wexler & Bar-El 2020). This division of labor, while sometimes overlapping, encourages bold experimentation across multiple fronts.

Private sector cybersecurity firms and Western intelligence agencies have uncovered evidence linking GRU units to advanced persistent threat groups that compromise space-related software and hardware (Wexler & Bar-El 2020; Theohary 2018). One well-known actor, often referred to as Turla, allegedly hijacks satellite-based internet links in developing regions to mask the origin of its attacks. Another example, Sandworm, is known for destructive malware targeting critical infrastructure in Ukraine and elsewhere. These groups illustrate Russia’s capacity to transform space infrastructure into both a cloak for offensive operations and a direct target for sabotage.

The war in Ukraine exemplifies how Russia integrates cyber operations in space with kinetic action. In 2014, as Russia annexed the Crimean Peninsula, it embarked on a series of network intrusions, jamming incidents, and disruptions aimed at crippling Ukraine’s command and control (Connell & Vogler 2017; Theohary 2018). By interfering with fiber-optic lines and hijacking communications, Russian forces limited the Ukrainian government’s ability to coordinate a rapid response. Pro-Russian hackers took down or defaced official websites, launched denial-of-service attacks, and spread disinformation to confuse Ukrainian citizens. Although it was not the first time Russia combined cyber tactics with traditional military force, 2014 revealed how satellite and telecommunications channels could be targeted to augment battlefield success.

In subsequent years, the contested region of Eastern Ukraine (particularly Donbas) became a testing ground for more sophisticated Russian cyber strikes. Russia jammed the Ukrainian military’s UAV data links, spoofed GPS signals to confound aviation routes, and deployed elaborate disinformation aimed at fracturing domestic support for Ukraine’s war effort (Adamsky 2018, Snegovaya 2020). International monitoring organizations attempting to oversee the conflict encountered jamming that made their drones inoperable, forcing them to rely on more limited ground-based observation. Each new incident underscored the strategic advantage that arises when an adversary loses confidence in its satellite positioning, weather data, or secure military communication.

By 2022, when Russia launched its renewed invasion of Ukraine, the reliance on offensive cyber measures was even more pronounced. Multiple accounts point to pre-invasion operations designed to compromise Ukrainian critical infrastructure. Immediately before the physical offensive, a destructive attack on the Viasat satellite network disrupted service for thousands of Ukrainian and European customers. The entire episode highlighted a broader principle: offensive operations on orbital assets or ground stations can cripple key systems instantly, creating confusion on the battlefield and slowing an adversary’s response.

Such methods derive from established Russian military doctrine. Theorists treat “information” not as a peripheral concern, but as a core element of modern warfare (Adamsky 2018; Snegovaya 2020). Consequently, the distinction between peace and war becomes blurred, since information confrontation is seen as continuous and persistent. Official documents typically frame cyber and space warfare concepts as purely reactive, defending Russia against the West’s perceived attempts to undermine its sphere of influence (Giles 2017; Connell & Vogler 2017). Yet the scale and sophistication of Russia’s cyber intrusions, especially those targeting foreign satellites, demonstrate a willingness to seize the initiative offensively. Researchers note that Russia invests heavily in ground-based anti-satellite weaponry, directed-energy systems, and co-orbital interceptors; still, it is the complement of cyber tools that makes these programs even more alarming (Raska 2020). Destroying a satellite with a missile invites global condemnation and orbital debris, whereas stealthy intrusions can degrade or compromise satellites without an overt demonstration.

The impetus for Russia’s offensive stance also springs from its particular economic and geopolitical position. Russia’s economy, heavily dependent on exports of raw materials, does not always match the innovation-driven profile of other major powers (Wexler & Bar-El 2020). In seeking to maintain “great power” status with fewer resources, Russia prizes cost-effective, asymmetric means that neutralize adversaries. Cyber operations against satellites offer a relatively low-cost path to strategic impact, allowing Russia to project influence beyond its regional environment (Connell & Vogler 2017; Baram & Bar-El 2019).

Within the doctrinal framework, Russia underscores synergy between electronic warfare, cyber warfare, and information warfare. It invests heavily in jamming equipment capable of disrupting or falsifying signals to satellites and UAVs. This synergy is evident not only in Ukraine but also in Syria, where Russian forces have tested jamming technologies against drones (Theohary 2018). Civilian shipping and aviation in these regions have reported erroneous GPS readings, consistent with advanced Russian hardware. Press reports and independent researchers have noted repeated anomalies near Russian facilities, especially around maritime ports, where vessels’ navigational instruments recorded inaccurate positions. Observers interpret these episodes as either tests of Russian capabilities or deliberate efforts to distort foreign intelligence collection.

Russia’s continuing emphasis on reflexive control further explains why disinformation and manipulation of perceptions operate in tandem with cyber sabotage. By infiltrating target networks, Russia can gather data about technical vulnerabilities as well as political fault lines. Then, it can deploy selective leaks, false narratives, or troll accounts on social media platforms to influence political discourse (Adamsky 2018). In a space-warfare context, the same reflexive control approach might involve denying satellite communications at critical moments in an adversary’s decision-making cycle, while releasing disinformation intended to sow discord among the adversary’s allies.

Assessments of Russian space-cyber operations frequently highlight well-publicized incidents of spoofing or jamming satellite systems (Raska 2020). In 2017, for instance, ships in the Black Sea reported contradictory GPS coordinates that placed them far inland at an airport. Similar anomalies were later detected in the Arctic region (Bilyana & Cheravitch 2020). While official Russian statements offered no explanation, many analysts believe Russia was actively spoofing signals to protect its own assets or test new capabilities. According to Russian strategic discourse, an opponent’s dependence on accurate satellite data is a critical vulnerability that Russia can exploit if necessary.

Despite its strong offensive dimension, Russia justifies these operations under a defensive narrative. Government statements and official doctrines mention foreign interference in Russia’s information space, alleging that Western governments sponsor protests, manipulate public sentiment, and orchestrate cyber-attacks on Russian systems (Giles 2021). The solution, in Moscow’s view, lies in strengthening internal control over data flows, promoting “digital sovereignty,” and preparing to respond to perceived aggression by taking down or crippling the adversary’s satellites, networks, and media channels (Snegovaya 2020).

Alongside these developments, Russia’s institutional reorganization has been notable. The Ministry of Defense, in concert with the General Staff, progressively integrated cyber specialists into new or existing units, while the GRU spearheads offensives abroad (Wexler & Bar-El 2020). Although attempts to form a centralized Cyber Command akin to the U.S. model have not fully materialized, the drive to unify these capabilities under a single strategic vision remains evident in policy directives (Bilyana & Cheravitch 2020). This looser structure, where distinct agencies overlap, encourages agility, as specialized teams can move quickly to exploit discovered vulnerabilities in foreign satellites or ground systems (Baram & Bar-El 2019).

By 2023, Russia has confronted the limits of these strategies in Ukraine, where resistance proved fiercer than anticipated and where Western powers provided extensive weaponry and intelligence to Kyiv. Nonetheless, Russia continues to leverage the full range of its cyber and space capabilities. Official messaging depicts the conflict as existential, justifying sophisticated cyber operations on Ukrainian infrastructure, both terrestrial and orbital, while threatening indirect harm to any outside actor that might intervene. Even as sanctions hamper Russia’s ability to collaborate on international space projects, the Kremlin consistently signals that if Western countries rely on satellites for intelligence, communications, or navigation, Russia can disrupt those assets in a crisis.

In conclusion, Russia’s offensive cyber strategy in the space domain is deeply intertwined with its broader tradition of information warfare, historical reliance on reflexive control, and need to maintain global influence despite economic constraints. The repeated combination of advanced cyber tools with kinetic operations, as demonstrated in Ukraine, underscores how Russia has fully embraced cyberspace as a mechanism for asserting power. If adversaries depend on satellites for situational awareness or troop coordination, Russia will seek to compromise those space assets and the ground stations that support them, often alongside disinformation campaigns that reinforce the impact of technical disruption. Whether these trends lead to further militarization of space or spark new regulatory initiatives, Russia’s current posture cements its reputation as a principal proponent of offensive cyberspace action against orbiting infrastructure.

* 1. ***China’s Cyber Strategy in Outer Space***

China’s space-cyber strategy arises from a distinctly different ideological and historical context compared to Russia, reflecting a confluence of Confucian traditions, Maoist thought, and modern Communist Party doctrines that emphasize social stability, economic development, and the safeguarding of national sovereignty (Kreps and Roggeveen 2016; Inkster 2019). While China indeed possesses an array of potentially offensive capabilities, it frames these primarily in preventive or defensive terms (Hoffman 2019). The People’s Republic of China (PRC) situates outer space within the larger concept of “informatization,” viewing integrated networks, satellites, and digital platforms as indispensable tools for projecting national power and sustaining economic progress (Kania 2016). Concurrently, Chinese doctrine underscores the avoidance of direct conflict where possible, especially if war would jeopardize long-term growth or undermine the Communist Party’s legitimacy (Segal 2018).

To appreciate China’s stance, one must first understand the reorganization of the People’s Liberation Army (PLA) around new domains. Since 2015, the PLA has prioritized integrating cyber, space, and electronic warfare capabilities within the Strategic Support Force (SSF) (Kania 2016). The SSF centralizes multiple aspects of information operations, enabling the Chinese military to streamline intelligence, communications, and counterspace efforts under a single command structure (Hoffman 2019). This transition was heavily influenced by lessons drawn from observing U.S. and NATO campaigns, where advanced satellite communications, real-time intelligence, and precision strikes proved decisive (Chase 2020). Chinese strategists concluded that achieving parity with the West required both robust space-based assets and matching denial capabilities (Bowe 2019).

Nonetheless, China’s guiding philosophy of “winning without fighting” resonates throughout its strategic documents and public statements (Feng 2005). Confucian heritage and Sun Tzu’s teachings have shaped an emphasis on indirect measures, sowing disunity among adversaries, using legal and psychological tools, and building diplomatic relationships. This preference for indirect action is modernized in the “three warfares”: public opinion warfare, psychological warfare, and legal warfare (Kania 2016). Although advanced cyber operations, including those aimed at satellites, are part of China’s operational repertoire, official doctrine emphasizes deterrence, denial, and espionage rather than overt destructive attacks.

China’s activities in the South China Sea illustrate these principles (Chase 2020). Beijing claims sovereignty over vast maritime areas and island features that are disputed by neighboring states. To consolidate its position, China has engaged in land reclamation, the deployment of military assets, and construction of dual-use facilities. Among the defense-oriented capabilities are electronic warfare units and radar installations that can jam or spoof GNSS signals. Vessels traveling in disputed waters have reported anomalies in their navigation data, indicating that Chinese forces are interfering with satellite signals to obscure their own activities or complicate foreign surveillance (Chase 2020).

Chinese officials characterize such measures as “preventive” or “defensive,” pointing to longstanding regional tensions and the need to protect maritime rights (Kreps and Roggeveen 2016; Inkster 2019). From Beijing’s perspective, denying foreign powers the ability to exploit satellite signals in these areas is an extension of sovereignty. Analysis of open-source imagery, along with intelligence leaks, reveals that China’s jamming apparatus in the South China Sea can be activated selectively, producing intermittent disruptions to navigation or reconnaissance systems. This measured and often covert approach reduces the risk of diplomatic escalation. While Russia makes headlines for dramatic interference, China generally opts for quieter methods.

A striking aspect of the Chinese approach is its relatively low public profile regarding actual counterspace operations. Whereas Russia engages in conspicuous demonstrations, China tends to downplay direct attacks on satellites. Although Beijing famously conducted an anti-satellite missile test in 2007, subsequent tests have been more discreet, sometimes cloaked as missile defense trials (Kania 2016). This posture reflects China’s intention to avoid incurring international condemnation or spurring open confrontation. Observers argue that China’s dual-use technologies, capable of intercepting ballistic missiles or satellites, are essential to the country’s aspiration for strategic autonomy (Segal 2018). Yet official statements reiterate a commitment to peaceful development, stressing that such capabilities will only be used if China’s core interests are seriously threatened.

Within Chinese strategic discourse, “cyber sovereignty” is also a central theme (Kreps and Roggeveen 2016). Much as Russia protects its domestic internet, China enforces strict controls over data flows, banning certain foreign platforms and requiring data localization. The underlying logic is that the state must regulate its digital ecosystem to preserve stability and reduce subversive risks. Extending these principles to space, China perceives satellites and orbital data as just another medium requiring secure management. By relying on its indigenous BeiDou navigation system, China eschews dependence on the U.S. GPS constellation and limits the possibility of external monitoring or disruption (Cheung 2017). BeiDou supports both the PLA and an array of civilian services, from smartphone mapping to logistics. This interplay of domestic cyber sovereignty with indigenous satellite systems enables China to conduct operations internationally without leaning on Western providers (Kania 2016; Hoffman 2019).

Espionage likewise plays a significant role in China’s approach to cyber warfare and space (Bowe 2019). Western agencies and cybersecurity researchers have documented extensive Chinese hacking campaigns targeting foreign defense contractors, satellite manufacturers, and aerospace research facilities. This intrusion presumably helps China close technological gaps more rapidly. In the satellite domain, infiltration of ground stations or supply chains yields not only technical secrets but also operational insights, informing Beijing on how best to disrupt or disable adversarial assets. Despite persistent accusations of state-sponsored hacking, China’s public stance is that it is a victim of foreign cyber aggressors, framing any recognized breach as necessary “self-defense”.

China’s economic motivations for a robust space-cyber stance stem from the importance of global trade routes, the Belt and Road Initiative, and ongoing domestic growth (Segal 2018). The South China Sea is viewed not just as national territory but as a vital maritime path for energy imports and exports Chase 2020). Maintaining strategic advantage in this region serves crucial economic interests. Chinese leaders remain aware that large-scale war could derail the country’s development agenda, undermining the Party’s legitimacy. They therefore prefer “offense-as-defense” only as a last resort, ensuring that any open conflict does not escalate to catastrophic levels.

In many ways, China’s approach to space cybersecurity mirrors its broader security thinking: incremental control, minimal provocation, and careful balancing of hard and soft power (Inkster 2019; Chase 2020). Analysts note that China rarely acknowledges offensive cyber operations publicly. The same restraint appears in official references to counterspace programs, which generally focus on deterrence, intelligence, and “active defense”. This posture aligns with the “three warfares,” whereby Beijing seeks to shape global narratives, casting China as a responsible power uninterested in reckless escalation, even as it acquires the means to sabotage adversaries’ satellites if needed (Feng 2005; Kania 2016).

Comparisons with Russia highlight notable organizational differences. Russia’s decentralized intelligence structure fosters overlapping missions, whereas China’s SSF constitutes a unified command that manages space-based assets, electronic warfare, and cyber units. China’s improved command organization is evident in testing and deploying systems that rapidly detect foreign satellites or missiles. By linking radars, data-processing centers, and the BeiDou network under the SSF, China ensures that relevant commands receive real-time awareness in a crisis. If foreign satellites attempt surveillance over the South China Sea or near Taiwan, SSF units could jam communications or deploy co-orbital interceptors (Chase 2020). That capacity, in turn, deters adversaries from challenging China’s territorial claims.

Another central element of China’s cyber approach is its reliance on legal and diplomatic frameworks. Beijing systematically uses international law, or its interpretations thereof, to legitimize maritime claims and justify defensive actions in orbital space (Inkster 2019; Bowe 2019). In public forums, Chinese officials highlight the importance of a “peaceful rise” and the need for new space governance measures to prevent orbital weaponization. Simultaneously, China remains cautious about treaties that would limit anti-satellite testing or the deployment of certain space assets. Beijing’s official stance is to support space demilitarization, but only insofar as it does not undermine its fundamental right to self-defense. From a Chinese perspective, the perceived militarization of U.S. space policy justifies the development of strong indigenous capabilities.

Case studies often point to 2019, when ships near the Spratly Islands reported unexplained GNSS disruptions (Chase 2020). Although China never officially acknowledged these actions, many assume PLA Navy or local electronic warfare units deliberately scrambled satellite signals to conceal Chinese installations. Similar patterns emerged in 2020–2021, with fishing fleets and research vessels encountering navigation errors. By maintaining a quasi-covert approach, China remains below the threshold likely to trigger direct retaliation. Such methods are ambiguous enough that technical glitches can be cited rather than open admission of jamming.

Another dimension pertains to technology transfer. Chinese academic and commercial cooperation with Western universities and firms extends to the aerospace sector (Bowe 2019). These partnerships foster technology diffusion that strengthens China’s capacity to develop dual-use space systems. The Belt and Road Initiative’s expansion into digital infrastructure, sometimes called the Digital Silk Road, coincides with broader satellite coverage, allowing China to offer communications services to partner nations. By doing so, China appears as a leader in global connectivity while reinforcing its own space-cyber security.

Despite its preference for caution, China’s planners acknowledge that controlling orbital environments is essential in a potential crisis over Taiwan or other core interests. Most analysts believe that in an extreme scenario, the PLA would quickly attempt to sabotage or jam U.S. and allied satellites (Kania 2016; Hoffman 2019; Chase 2020). Yet official Chinese statements rarely detail such offensive tactics, preserving ambiguity that might deter foreign intervention. In Chinese strategic culture, this duality, capability plus caution, serves primarily to prevent conflict rather than encourage it.

In short, China’s cyber strategy for space revolves around denying adversaries unfettered satellite access, strengthening Beijing’s own capabilities, and managing the global narrative so that any actions appear purely defensive. Through the SSF, China integrates technical prowess, intelligence, and hardware for potential showdowns. By controlling digital spaces domestically, the Party ensures minimal internal subversion and stable public opinion. Although China presents itself as a defensive actor, evidence of advanced technology and operational patterns indicates strong offensive or preemptive potential.

Over the coming years, China’s strategy may yield a dynamic interplay of competition and collaboration with other space powers. On one hand, China continues civilian space cooperation, such as Earth observation and climate research; on the other, it remains poised to disrupt or deny foreign satellites if needed. By tying economic initiatives to technical mastery, China portrays itself as a technologically advanced nation open to global partnerships, while discreetly retaining a capacity to degrade rivals’ orbital assets at a moment’s notice.

1. **Discussion**

The findings from the Russia and China case studies demonstrate how both powers engage in significant cyber activities related to satellites and orbital networks, yet they diverge in approach, rhetoric, and operational emphasis. Russia foregrounds offensive measures, frequently tested and demonstrated in military conflicts, whereas China espouses what it labels defensive or preventive policies, though its capabilities are sophisticated enough to conduct offensive operations if deemed necessary. By reflecting on similarities and differences in these cases, we can explore what drives variations in space-cyber strategy, why ideology and strategic culture matter, and the implications for international security.

A central point emerging from both case studies is that technology alone does not determine how a state uses cyber means in outer space. Instead, national ideologies, historical traditions of warfare, and strategic cultures heavily influence these decisions (Piotrowski 2019; Johnson 2023). In Russia’s case, concepts inherited from the Soviet era, foremost among them the idea of reflexive control, continue to infuse official doctrine and day-to-day operations. Reflexive control, understood as manipulating an adversary’s perceptions to induce advantageous behavior, naturally lends itself to offensive uses of cyber tools. Especially in times of heightened geopolitical tension, such as the conflict in Ukraine, Russia’s government appears prepared to degrade or disrupt satellite infrastructure, employing the logic that controlling an opponent’s flow of information reduces that opponent’s capacity for coherent response.

China, too, draws on an extensive ideological and historical background, including Confucian and Sun Tzu-inspired emphases on indirect warfare, political unity, and the preservation of harmony. Overlaying these philosophical traditions is the modern Chinese Communist Party (CCP) framework, which prioritizes domestic stability, economic development, and social order. Consequently, Beijing’s official line on cyberspace in orbit highlights a “peaceful development” model, claiming only to deny adversaries capabilities that threaten China’s “core interests.” Observers interpret such an approach as an outgrowth of China’s preference for incremental power acquisition, shaped by the “three warfares” (public opinion, psychological, and legal) that emphasize shaping the environment before engaging in a shooting war.

These divergent ideological underpinnings help explain why each superpower’s rhetorical justification for its space-cyber activities differs markedly, even as the practical effects, spoofing, jamming, or infiltration, may bear superficial resemblance. Russia readily deploys disinformation campaigns and physically disruptive actions, while publicly framing them as defensive responses to “Western aggression”. China, by contrast, emphasizes a posture of “active defense,” frequently referencing external legal frameworks and the pursuit of “cyber sovereignty” to justify controlling or denying space-based services in disputed areas. Such stances demonstrate that space-cyber strategies cannot be reduced to hardware and engineering capacities; they are deeply woven into each nation’s broader strategic worldview.

Although the case studies categorize Russia’s strategy as “offensive” and China’s as “defensive/preventive,” the reality is more nuanced, as is often the case with such categorizations (Gilli & Gilli 2019; Grand 2020). Both powers can and do conduct espionage in orbit, both invest in directed-energy research and co-orbital interception vehicles, and both have tested anti-satellite (ASAT) systems. Hence, each superpower already wields the capacity to degrade or destroy adversarial satellites if required. The difference lies less in the sheer availability of these technologies and more in how and when each superpower is inclined to use them. Russia’s use of offensive cyber measures in space is highly visible, particularly in the context of active military campaigns. Several documented incidents in Ukraine exemplify large-scale jamming, spoofing, or hacking of critical infrastructure that depends on satellite communications. By contrast, China has largely avoided conspicuous sabotage in overt conflicts, focusing instead on incremental, sometimes covert, denial within contested zones like the South China Sea. Russia’s approach is shaped by a strategic culture that frames all forms of international engagement as information warfare, ongoing and inherently conflictual. China’s approach is characterized by a deeply held desire to sustain stability for economic progress, using denial as a deterrent more than as an immediate instrument of warfare.

Still, the gap is narrower than official statements might suggest. China, despite rhetorical commitments to peaceful use, invests heavily in technologies capable of neutralizing satellites, through either direct kinetic attacks or sophisticated cyber intrusions. Russia, despite its aggressive posture, also frames its actions as “defensive,” claiming it is compelled by the West’s perceived encroachments. Thus, both states, in effect, practice an offense-defense mix that depends on context. Russia is more willing to demonstrate real-time disruption, China more content to maintain the capacity for disruption without employing it as visibly. The difference in public performance shapes global perceptions of these two powers but does not necessarily indicate that one is incapable of the other’s methods.

A unifying theme is the desire for asymmetric leverage to counter a perceived technologically superior adversary, namely, the United States. Both Russia and China view American space assets as central to Western military dominance, from precision-guided munitions to global surveillance. Developing space-cyber capabilities that can undermine or threaten U.S. satellites is therefore a rational and cost-effective pathway to offset that dominance. For Russia, the combination of economic constraints and a historical tradition of matching or outmaneuvering Western powers motivates the pursuit of advanced cyber and electronic warfare. For China, the impetus is the imperative to prevent foreign interference in what it regards as sovereign territory, while simultaneously avoiding escalation that could derail its economic modernization.

Deterrence also factors heavily into both countries’ strategies. If an adversary believes its orbital resources, communications, navigation, or observation satellites, might be neutralized, it may hesitate before challenging Russian or Chinese interests. In other words, by demonstrating at least some measure of offensive readiness, both Moscow and Beijing hope to dissuade others from direct confrontation in domains they deem essential. This logic is particularly evident in China’s approach to Taiwan and the South China Sea, where the mere presence of jam-capable facilities might prevent foreign powers from fully leveraging space-based assets in a crisis.

Yet deterrence in space-cyber operations is complicated by the difficulty of attribution and the relative invisibility of certain actions (Goldman & Warner 2022; Wheeler 2021). A missile-based ASAT attack is obvious and trackable, whereas a cyber intrusion on a satellite’s software can be masked or denied. Thus, states may feel emboldened to try covert measures in pursuit of strategic advantage, expecting that attribution challenges will diminish the risk of retaliation. Russia’s repeated intrusions in Ukraine, for example, rarely elicit immediate, overt counterstrikes from foreign adversaries, in part because such covert activities remain murky in terms of formal blame. For China, denial by jamming or spoofing can often be denied altogether, allowing it to push boundaries without openly provoking a crisis.

An additional driver of the observed divergence is the structural and institutional environment in which each superpower’s space-cyber strategy evolves. In Russia, the absence of a single, unified cyber command means that multiple security agencies, the GRU, FSB, and SVR, operate in overlapping or sometimes competing spheres. This environment fosters bold experimentation and a degree of institutional rivalry, as different units within the military or intelligence community seek to achieve high-impact results to demonstrate their utility to political leaders. Hence, the “offensive patchwork” approach emerges from a more decentralized system that can quickly adapt to discovered vulnerabilities in foreign satellite networks.

China, by contrast, consolidated its space, cyber, and electronic warfare capabilities under the Strategic Support Force (SSF) starting around 2015. This structure promotes a coordinated approach in which intelligence, research, and operational units align under a single command. The SSF’s emphasis on synergy and unified planning helps Beijing maintain a coherent vision of denial and preemptive defense. While it is not immune to bureaucratic politics, the Chinese system aims to reduce duplication and present a tightly managed front, consistent with the broader CCP model of top-down governance.

Hence, when analyzing operational outcomes, it is clear that Russia’s decentralized approach sometimes yields dramatic intrusions, while China’s relatively centralized approach prioritizes integrated planning and discreet denial. Each structural arrangement reflects larger differences in political organization. Russia, historically, was comfortable mixing formal structures with informal “patriotic hacker” groups, while China’s CCP fosters a disciplined hierarchy even in cyberspace. These institutional choices shape how each state designs, tests, and executes space-cyber missions.

A further dimension requiring attention is the widespread use of “information warfare” in both countries but to somewhat different effect. Russia’s concept of information confrontation embraces the tactical, technical, and psychological realms almost equally, merging disinformation campaigns and sabotage efforts to destabilize rival states internally while degrading their technical infrastructure. This integrated approach is especially visible in Ukraine, where misinformation about events on the ground often coincides with satellite or radio jamming, hindering the Ukrainian military’s communication and muddying the public’s understanding of the situation.

China’s approach to information warfare is likewise multi-faceted but more oriented toward deterrence and prevention. Beijing manipulates narratives in contested regions such as the South China Sea by emphasizing historical claims and legal arguments. At the operational level, jamming or spoofing satellite signals complicates foreign naval or aerial surveillance, but rarely is it accompanied by brazen public disinformation designed to foment domestic unrest in an adversary state (Cheung 2017). The Party’s strategic emphasis on preserving internal stability and avoiding large-scale conflict influences how it wields information warfare. If deception or psychological manipulation is employed, it often seeks to create ambiguity about the region’s status rather than openly destabilize a rival’s government.

Despite these distinctions, both superpowers recognize the potency of shaping the adversary’s perceptions, be it domestic or international audiences. In Russia’s case, the synergy of reflexive control with real-time sabotage can yield quick strategic dividends, but at the cost of international condemnation when the operations are uncovered (Bilyana & Cheravitch 2020). In China’s case, quietly executed jamming or spoofing might achieve strategic denial with minimal reputational cost, especially if plausible deniability is maintained (Hoffman 2019). Each model is consistent with a broader worldview: Russia openly contests Western narratives, seeing itself in an enduring struggle with the West, whereas China blends subtlety with official discourse emphasizing “peaceful rise” and “win-win cooperation”.

One of the most pressing findings from these comparative case studies is that space-cyber operations introduce a new layer of ambiguity and risk in international security (Pavur and Martinovic 2019). Neither Russia nor China acknowledges their own tactics as aggressive or escalatory, portraying them instead as measured responses to external threats (Piotrowski 2019; Johnson 2023). Yet their readiness to degrade or disrupt satellites can impose severe costs on civilian infrastructure, including telecommunications, navigation services, financial transactions, and emergency response systems. A large-scale jamming attack or a malicious intrusion on satellite software could cause massive economic damage and public safety hazards, far beyond conventional military targets.

Moreover, there is no comprehensive legal framework that adequately addresses cyber operations in space (Falcão Serra 2021; Meyer 2016; Sadeh 2010). Existing treaties, like the Outer Space Treaty, speak to the peaceful use of outer space but lack explicit definitions or enforcement mechanisms for cyberattacks on satellites. Russia and China both advocate certain arms control measures in orbit but remain vague about how these would apply to non-kinetic disruptions, such as hacking ground stations or injecting malware into satellite software.

Additionally, attributing cyber incidents in orbit is even more challenging than attributing terrestrial hacking, due to limited transparency and the cross-border nature of satellite communications (Goldman & Warner 2022; Wheeler 2021). The net result is a precarious environment in which states can (and sometimes do) carry out clandestine sabotage with potentially global repercussions, all without breaching any widely recognized “red lines.” A miscalculation in this domain could escalate conflicts unexpectedly, particularly if a major power’s critical space assets appear to be under attack. In the absence of clear norms or confidence-building measures, each side might assume worst-case intentions (Grand 2020; Wheeler 2021). Russia’s established record of brazen offensives, paired with China’s preference for subtle denial, amplifies the risk of mistrust and misinterpretation.

In exploring why Russia and China pursue such distinct approaches, we see that each superpower’s strategy is informed by its historical experience, political-economic context, strategic culture, and institutional configuration. Russia’s legacy of total warfare, reflexive control, and ideological confrontation with the West shapes its willingness to operate offensively. China’s tradition of layered deterrence and Confucian emphasis on order influences its emphasis on shaping the environment and avoiding open conflict. Russia’s resource-based economy and desire for global influence despite fewer resources lead to a reliance on low-cost, high-impact cyber operations. China’s economic strategy of steady growth and international trade alliances prompts it to minimize provocative actions that could disrupt global markets or alliances/ Russia’s strategic culture frames cyber, space, and conventional capabilities as intertwined in a perpetual information war, while China’s strategic culture, especially with the three warfares, emphasizes controlling narratives and deflecting direct military showdowns. Finally, Russia’s decentralized intelligence and security landscape fosters relatively rapid, if sometimes chaotic, offensive operations, whereas China’s centralized SSF supports unified command of space, cyber, and electronic warfare, reinforcing a measured, integrated denial approach.

Synthesizing these elements leads to the conclusion that the perceived differences between Russia’s “offensive” stance and China’s “defensive” one reflect deeper structural and cultural factors rather than raw differences in capability. Both states want to disrupt adversaries if necessary, both invest in advanced anti-satellite means, both depict their measures as fundamentally defensive, and both seek to leverage the inherent ambiguity of cyberspace to avoid overt blame.

These findings highlight lessons for policymakers concerned about the militarization of outer space, including the need for clarity and norms regarding non-kinetic operations, the importance of attribution mechanisms that reduce the confusion arising from covert actions, the influence of domestic politics and culture, and the potential for escalation in regional disputes. As the Russia-Ukraine conflict and the South China Sea tensions illustrate, space-cyber actions can quickly spill into broader confrontations, leading to sudden satellite outages or data manipulations that introduce confusion in crisis management. Commercial satellite providers also become targets, exemplified by the Viasat intrusion in Ukraine. Efforts to mitigate escalatory risks must thus address not only hardware protections but also the policy rationales driving Russia and China to adopt these strategies. For researchers, these cases open avenues for further comparative work, revealing how middle powers may follow similar patterns or develop variations aligned with their own strategic cultures. It is plausible that the approaches taken by states such as India, Iran, or North Korea reflect unique blends of ideology, history, and capacity.

Both Russia’s and China’s approaches to space-cyber issues continue to evolve. Technological leaps, such as the proliferation of small satellites and the rise of private space companies, alter the threat environment. Russia and China adapt to these shifts in light of their respective goals, domestic priorities, and perceptions of Western strategies. Russia’s direct experiences in Ukraine may lead to further integration of cyber sabotage with ground operations, while China refines large-scale electronic warfare and cyber denial around its critical regions, trusting that the SSF can coordinate these efforts discreetly. Observers should not assume that either superpower is locked into its current stance indefinitely; domestic political pressures, leadership changes, and foreign policy realignments could all reshape how they handle space-cyber matters.

Policymakers must therefore recognize that states’ ideological outlooks and strategic histories cannot be divorced from their operational decisions. The task of mitigating escalatory risks in orbit demands not only technical solutions, such as robust satellite design or improved attribution, but also deeper diplomatic engagement that addresses the underlying motivations for offensive or preventive space-cyber maneuvers. By examining these rationales, the global community may be better positioned to devise frameworks that reduce the likelihood of a space-cyber crisis with cascading effects on economic stability, international peace, and the broader world order in the twenty-first century.

1. **Conclusions**

This article has demonstrated that Russia’s and China’s divergent cyber strategies in space reflect their broader traditions of security, ideology, and statecraft. Although both states possess sophisticated space-based intelligence, electronic warfare, and hacking methods, Russia consistently displays a more offensively oriented posture, employing sabotage, disinformation, and direct cyber-attacks on adversary infrastructure, even during combined arms offensives. China, by contrast, invokes a preventive or defensive framing of space-cyber activity, focusing on electronic jamming and denial to preserve regional military advantage and deter foreign intervention. This difference stems from ideological underpinnings, ranging from Soviet reflexive control to Confucian emphasis on stability, as well as from the distinct geopolitical goals each state prioritizes.

The findings affirm that Russia’s offensive posture is not merely the product of advanced technology or opportunism; it arises from a strategic culture that regards cyberspace as a theater of permanent confrontation. China, for its part, prioritizes economic advancement and domestic governance, preferring to wield space-cyber capabilities in ways that protect its current trajectory without risking severe conflict escalation. While each nation consistently intensifies and modernizes its presence in space, neither appears fully mindful of the potential for catastrophic miscalculation in the absence of internationally agreed norms. The consequences of advanced cyber operations in space could be immense, impairing critical services for millions of people and setting dangerous precedents for militarizing outer space.

Policymakers worldwide may draw several lessons from this comparative analysis. First, space-cyber attacks are likely to remain an attractive option for major powers seeking strategic advantage without overt escalation. Second, measures to foster transparency and confidence-building in space are lagging behind the rapidly evolving capabilities of Russia, China, and others. Finally, attempts to restrict or regulate destructive cyber operations against satellites should address the underlying ideological motives that can incentivize such methods. Simply controlling hardware proliferation or restricting ballistic anti-satellite tests will not suffice if states remain committed to clandestine sabotage as a tool of grand strategy. Consequently, forging any lasting arms control or governance framework in space will require a deeper understanding of how states conceptualize information warfare itself, and whether they believe that escalatory cyber actions serve or endanger their national interests.

**References**

Adamsky, Dmitry. 2018. “Cross-Domain Coercion: The Current Russian Art of Strategy.” IFRI Security Studies, no. 48.

Agentura (2022) Overview of Russian Cyber Agencies. Retrieved from Agentura.ru (in Russian).

Aviv, Y., & Ferri, P. (2023) “Wiper Malware and Hybrid Warfare in the Russia-Ukraine Conflict,” Journal of Cyber Conflict Studies, 43.

Baram, G., & Bar-El, B. (2019) “Between Offensive and Defensive: Characterizing Information Warfare in the 21st Century,” Comparative Strategy, 94-102.

Bilyana, L., & Cheravitch, E. (2020) “Russian Military Thought: Concepts and Elements of Information Confrontation,” Journal of Slavic Military Studies.

Bowe, Alexander. 2019. China’s Overseas United Front Work: Background and Implications for the United States. Washington, DC: U.S.-China Economic and Security Review Commission.

Chase, Michael S. 2020. China’s Space and Counterspace Capabilities and Activities. Santa Monica, CA: RAND Corporation.

Cheung, Tai Ming. 2017. “The Chinese Defense Economy’s Long March from Imitation to Innovation.” Journal of Strategic Studies 40 (2): 225–248.

Cohen, B., & Bar-El, R. (2017) “Offensive Cyber Operations and Control of Information,” Defense & Security Analysis, 14-15.

Connell, Mary, and Sarah Vogler (2017) Russia’s Approach to Cyber Warfare. Arlington, VA: CNA.

Coultrup, G. (2022) “GNSS Disruptions in Northern Norway,” Electronic Warfare Quarterly.

CyberPeace Institute (2022) “Cyber Attacks against Satellite Infrastructure in the Russia-Ukraine War,” CyberPeace Brief.

Eriksson, J., & Privalov, A. (2021) “Russia’s Space Program in the 21st Century: Between Legacy, Militarization, and Modernization,” Space Policy 24: 381–407.

Falcão Serra, João (2021) "Cybersecurity and Outer Space: Learning from Connected Challenges." *Outer Space and Cyber Space: Similarities, Interrelations and Legal Perspectives*: 87-103.

Falco, G. (2018) “Job One for Space Force: Space Asset Cybersecurity,” Bulletin of the Atomic Scientists.

Febbraro, Daniella (2023) "The Need for Cyber Resilience of Space Assets: Law and Policy Considerations of Ensuring Cybersecurity in Outer Space." *Canadian Journal of Law and Technology* 21, no. 1: 99.

Feng, H. (2005) “A Dragon’s Approach to Information Warfare: Methodologies and Doctrine,” Journal of Contemporary China 14:637-662.

Giles, Keir (2017). Handbook of Russian Information Warfare. London: Chatham House.  
  
Giles, Keir. 2021. “Russia’s War on Information.” Survival 63 (3): 7–14.

Gilli, Andrea, and Mauro Gilli. 2019. “Military-Technological Superiority, Systems Integration, and the Challenges of Imitation.” *International Security* 43 (1): 141–189.

Gleason, G. (2018) “Digital Sovereignty in Russian Policy,” Orbis 15(36).

Goldman, Emily O., and Michael Warner. 2022. “Attribution in Cyberspace and Outer Space: Shared Dilemmas, Divergent Solutions.” *Cyber Conflict Review* 3 (2): 81–99.

Grand, Camille. 2020. “Arms Control and Non-Kinetic Threats in Outer Space.” *Survival* 62 (5): 97–105.

Greenberg, A. (2018) “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired.

Guchua, L. et al. (2022) “Cyber Dimensions of Modern Warfare: A Case Study of Russia-Ukraine,” Conflict and Security 10: 27–36.

Guliyeva, A. (2021) “Cyber Strategies in Russia’s Foreign Policy,” Russian Studies Review (in Russian).

Hambling, D. (2017) “First Evidence of GPS Spoofing? Black Sea Mystery,” New Scientist.

Hoffman, S. (2019) “China’s Cyber and Space Capabilities: Probing the Gray Zone,” Asian Security 42(1).

Hurska, A. (2022) “Pre-Invasion Cyber Operations in Ukraine,” Cyber Defense Analysis.

Inkster, Nigel. 2019. The Great Decoupling: China, America and the Struggle for Technological Supremacy. London: Routledge.

Johnson, James. 2023. “Dangerous Confidence? Chinese and Russian Perceptions of Technological Superiority and Escalation in the Gray Zone.” *Journal of Strategic Studies* 46 (1): 1–21.

Kania, E. (2016) “The PLA Strategic Support Force and Future Chinese Warfare,” China Brief 16(13).

Kostiuchenko, V. et al. (2021) “Russia’s Federal Space Program and Military Integration,” Defense Perspectives (in Russian).

Kreps, Sarah, and Sam Roggeveen. 2016. “In the Realm of the Senses: The Socialization of Chinese Cyber Strategy.” Journal of Strategic Studies 39 (1): 113–136.

Kube, C. (2018) “Russia Jamming U.S. Drones in Syria,” NBC News.

Lennon, S. (2015) “The Turla Group’s Satellite Hijacking Tactics,” Kaspersky Lab Security Bulletin.

Li, Du (2023) "Cyber-attacks on space activities: Revisiting the responsibility regime of article vi of the outer space treaty." *Space Policy* 63: 101522.

Luzin, P. (2023) “Russia’s Space Budget and Reorientation Post-2022,” SpaceWatch Global.

Maini, A. K., & Agrawal, V. (2014) Satellite Technology: Principles and Applications. Hoboken: Wiley.

Manulis, M., Bridges, J., Harrison, K., Sekar, V., & Davis, G. (2020) “Cybersecurity of Satellite Ground Stations,” Satellite Communications Review 1-25.

Martin, Anne-Sophie (2023) "Outer space, the final frontier of cyberspace: Regulating cybersecurity issues in two interwoven domains." *Astropolitics* 21, no. 1: 1-22.

Martti, J. (2019) “Russian Strategic Culture and Cyber Warfare,” Journal of Strategic Studies: 91.

Maurer, T. (2015) “Cyber Proxies and the Crisis in Ukraine,” in Cyber War in Perspective: Russian Aggression against Ukraine.

Meyer, Paul (2016) "Outer space and cyberspace: A tale of two security realms." *International Cyber Norms: Legal Policy & Industry Perspectives*: 155-169.

Mikhlin, V., et al. (2019) “The Evolution of Information Warfare in Russian Military Thought,” Journal of Contemporary Security Studies 247.

Paikowsky, D. (2017) The Power of the Space Club: The Global Impact of Outer Space on the World Order. Cambridge University Press.

Pavur, James, and Ivan Martinovic (2019) "The cyber-ASAT: on the impact of cyber weapons in outer space." In *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, pp. 1-18. IEEE.

Piotrowski, Marcin Andrzej. 2019. “Russia’s Information Warfare and Cyber Strategy.” *Polish Institute of International Affairs (PISM) Report.* Warsaw: PISM.

Reesman, R., & Wilson, J. (2020) “Geopolitical Shifts and the Future of Lunar Exploration,” Aerospace Policy Report.

Racionero-Garcia, Juan, and Siraj Ahmed Shaikh (2024) "Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives." *Space Policy*: 101648.

Raska, Michael. 2020. “Strategic Contours of Russian Cyber Warfare.” International Journal of Cyber Warfare Studies 5 (2): 73–91.

Sadeh, E. (2010) “Governance of Space: Regulating Cyber Capabilities in Orbit,” Space & Polity 8(2–3): 73–112.

Segal, Adam. 2018. The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. New York: PublicAffairs.

Shahzad, H., Qiao, L., & Joiner, T. (2022) “Satellite Vulnerabilities to Cyber Threats,” Journal of Space Security 17(1):404–412.

Sharikov, P. (2018) “Sovereign Internet and Russian Information Security,” Russian Politics & Law.

Snegovaya, Maria. 2020. Putin’s Information Warfare in Ukraine: Soviet Origins of Russia’s Hybrid Warfare. New York: Council on Foreign Relations.

Sunghwan, L. (2022) “Evaluating Russia’s ASAT Tests and Anti-Satellite Laser Capabilities,” Korean Defense Analysis (in Korean).

The White House (2020) Executive Order on Strengthening National Resilience through Responsible Use of PNT Services.

Theohary, C. (2018) “Information Warfare: Issues for Congress,” Congressional Research Service.

Weeden, B. & Samson, V. (2019) Global Counterspace Capabilities: An Open Source Assessment. Secure World Foundation.

Wexler, H. & Bar-El, B. (2020) “Russia’s Cyber Force Structure: From Decentralization to Global Disruption,” International Security Review.

Wheeler, Tarah. 2021. “Resilience in the Commercial Space Sector: Risks and Opportunities in Cybersecurity.” *Cyber Defense Journal* 4 (3): 10–28.