How Ends, Ways, and Means are Manifested in the Cyber Defense Strategies of Superpowers

Piia Perälä, Martti Lehto and Pekka Pirinen
Faculty of Information Technology, University of Jyväskylä, Finland

piia.m.h.perala@jyu.fi
martti.j.lehto@jyu.fi
pekka.j.pirinen@jyu.fi

Abstract: Cyber Power refers to the capacity to project and promote national interests in and through cyberspace. The military contributes to multiple aspects of cyber power, with cyber warfare capabilities being a central component. Numerous state and non-state actors have come to regard cyber ends, ways and means, as a powerful force multiplier, essential to achieving their objectives. Military cyber actors employ malicious cyber operations to gain asymmetric advantages, targeting critical infrastructure and undermining the opponent's military superiority in cyberspace. The development of cyber warfare has seen a convergence with other non-kinetic warfare operations. Superpowers adopt distinct approaches to cyber warfare, with varying definitions, strategic objectives, and methods for achieving them. They have also established their own command structures and cyber forces. This paper aims to provide an understanding of how superpowers use cyber capabilities and leverage asymmetric advantages to achieve their strategic objectives. The research material consisted of publicly available documents on national strategic cyber defense plans. Lykke's framework was applied as a structured approach to review superpowers' strategic plans by identifying the desired outcomes (Ends), the methods used to achieve them (Ways), and the resources required (Means).

Keywords: Superpowers, Cyber warfare, Ends, Ways, Means, Convergence, Cyber defense strategy, Cyber power

1. Introduction

Cyber power is the ability of a state to advance national interests through cyberspace. Military cyber capabilities form a core component of this power, as cyber warfare has become a critical tool for achieving strategic objectives. (Voo *et al.*, 2020) States and non-state actors increasingly view cyber operations as force multipliers, enabling asymmetric advantages. Cyber warfare has converged with other non-kinetic domains, challenging traditional concepts of conflict (Lehto and Limnéll, 2017). Nations have developed distinct approaches to cyber warfare, shaped by their strategic cultures, political systems, and technological capabilities. Definitions of cyber warfare and its objectives vary across nations, as do the ways to achieve goals (Giles, 2021). While some nations prioritize technical dominance and infrastructure resilience, others emphasize cognitive influence and information control.

This paper aims to provide an understanding of how the cyber superpowers, namely the United States (US), Russia, and China, employ cyber capabilities to achieve strategic objectives. Applying Lykke's framework, we analyzed publicly available documents outlining these nations' strategic cyber defense plans, aiming to identify their cyber defense ends, ways, and means. The paper provides insight into how these superpowers leverage cyber capabilities and asymmetric advantages to accomplish their strategic objectives.

2. Cyber Warfare, Power, and Deterrence

2.1 Cyber Warfare

Since the 1990s, cyber warfare has emerged as a parallel domain to traditional kinetic warfare, often complementing conventional military operations (Haizler, 2017). It is a key element of hybrid warfare, which combines military force, irregular tactics, and criminal activities by state or non-state actors (Lalu and Puistola, 2015). Cyber warfare has challenged the traditional paradigm of warfare. Operating in the cyber environment has reduced the relevance of formal declarations of war or peace. In cyberspace, conflicts lack clear beginnings or endings, resulting in prolonged periods of instability for targeted entities. (Lehto and Limnéll, 2017)

Defining cyber warfare is challenging, as no universally accepted definition exists (Haizler, 2017). The term broadly covers diverse activities in the cyber domain, yet certain common characteristics can still be identified. Cyber warfare operates in a borderless digital battlespace with no front lines, exposing both military and civilian systems. Its rapid tempo shifts conflicts to seconds, and its impact reaches critical infrastructure and public services. Cyber-attacks target both virtual systems and physical hardware, aiming for systemic disruption rather than isolated damage. Often integrated with kinetic and hybrid warfare, these operations combine cyber, information, and electronic tactics. Cyber operations can occur without formal declarations of war, typically by

state or state-sponsored actors, making cyber threats persistent and low-threshold in modern conflict. (Lehto and Limnéll, 2017)

2.2 Cyber Power

In the modern world, cyber capabilities have become a key element of national power (IISS, 2021). Cyber power enables states to achieve strategic objectives through cyberspace, with military applications playing a central role (Voo *et al.*, 2020). Definitions converge on the idea that cyber power is a state's ability to leverage cyberspace to influence outcomes and pursue goals (Kuehl, 2009; Nye, 2010; Voo *et al.*, 2020). Cyber power is shaped by technology, organizational structures, and user capabilities. Its development and application are influenced by national missions, such as military, economic, or political (Kuehl, 2009). It can affect both digital and physical domains and serve strategic or political aims (Lehto and Limnéll, 2017). Unlike traditional power, cyber power is not dependent on a state's size or proximity. Instead, it hinges on clear objectives, the means to achieve them, and leveraging cyber means to accomplish multiple objectives. (Lehto and Limnéll, 2017; Voo *et al.*, 2020).

2.3 Cyber Deterrence

While cyber deterrence typically operates within the cyber domain, its effects can extend beyond it (Lonergan and Montgomery, 2021). Effective deterrence depends on a credible threat that convinces potential attackers the costs outweigh the benefits. States adopting this strategy may not seek conflict but remain prepared to defend vital interests if necessary (Pijpers and Arnold, 2025). According to Lehto and Limnéll (2017), building cyber deterrence requires the ability to defend society broadly in the cyber environment, tolerate attacks effectively, and attribute the source of those attacks. States must also be capable of launching counterattacks and responding through political means when needed. A sufficient level of cyber self-sufficiency and competence is essential. Public communication strengthens cyber deterrence. Although cyber capabilities are often classified, states may disclose or demonstrate certain capabilities to enhance credibility (Limnéll, 2013).

3. The US, Chinese, and Russian Approaches to Warfare in Cyberspace

The US military defines cyberspace as “a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (US DoD, 2021, p. 55). Cyber operations involve using these capabilities to achieve objectives within or through cyberspace, while cyber warfare refers to armed conflict conducted partly or wholly via cyber means. Its goal is to deny adversaries the effective use of cyberspace systems and includes attacks, defense, and enabling actions (US DoD, 2010). Unlike the US's technical and infrastructure-focused view, China and Russia adopt broader approaches. China views the information space as a global communication domain, aligning with Russia’s concept of a cognitive space involving human information processing (Giles and Ii, 2013).

China treats information as a distinct domain of warfare, equal to land, sea, air, space, and cyber, with a strong focus on ideological control and perception management (Giles and Ii, 2013). Its concept of information spans cyberspace, the electromagnetic spectrum, physical infrastructure, and the cognitive domain (Mulvaney, 2025). China emphasizes the close link between space and cyber, viewing both as extensions of the electromagnetic spectrum (Costello and McReynolds, 2018). China perceives peace and war as a continuum, not separate states, and integrates offensive cyber operations into a broader strategy of information warfare that spans military, diplomatic, and economic spheres. Like Russia, China combines cyber capabilities and information warfare, emphasizing the fusion of multiple warfare types utilizing information technologies. Its cyber strategy is tied to social stability and military modernization. (Pusztaszeri, Harding and Dickson, 2025) The development of an ‘informatized’ and ‘intelligentized’ military through ‘digitization’, ‘networkization’, and AI-driven smartification is central to the evolution of the People's Liberation Army (PLA) doctrine and future conflict readiness (Mulvaney, 2025).

Russia considers cyber and information operations inseparable, framing its activities under the concept of ‘information confrontation’. This approach encompasses a broader and continuous range of actions than the US notion of cyberwar, extending beyond wartime operations (Dickson and Harding, 2025). Information confrontation includes both technical and psychological dimensions, with cognitive operations playing a central role in shaping public perception and influencing decision-making (Hakala and Melnychuk, 2021). Russia avoids the term ‘cyber warfare’ and, together with China, shares the understanding that it describes foreign concepts, mainly Western threats and activities (Giles and Ii, 2013).

4. Lykkes' Framework

In 1989, Colonel Arthur F. Lykke Jr. presented a model concerning military strategy. Lykke's (Lykke, 1989) model suggests that military strategy, or any other strategy (e.g., political, economic etc.), can be viewed as an equation in which ends, ways, and means form the strategy. Ends refer to the objectives to be achieved. Ways describe the actions that need to be taken to reach the goals, and means are the resources required to achieve the ends. These strategic concepts support approaches at all levels: strategic, operational and tactical. Applying Lykke's model to cyber defense strategies, 'ends' refer to strategic objectives such as defending against cyber threats. 'Ways' refers to the methods used (e.g., disrupting malicious actors), and 'Means' refers to the required resources (e.g., skilled personnel, funding, and advanced cyber tools).

5. Method

The research material consisted of publicly available documents outlining strategic cyber defense plans of the US, Russia, and China. The appropriateness of the documents was evaluated against four criteria (Scott, 2014): authenticity, credibility, representativeness, and meaning. For example, we reviewed document details (e.g., authors, publishers, affiliated organizations, and publication year) to ensure authenticity and confirm that the documents were from credible sources. We also ensured that the content was relevant to our study aims. Only documents written in languages understood by the authors were included.

For the analysis, we used thematic analysis (Braun and Clarke, 2012) and applied Lykke's (1989) framework to identify key concepts: ends, ways, and means. We began the analysis by familiarizing ourselves with the research materials, after which the data was coded and features corresponding to Lykke's concepts were identified. We utilized Atlas.ti for coding. Codes that shared common characteristics were clustered to generate themes and sub-themes.

6. Ends, Ways, and Means of Superpowers in Cyber Defense

6.1 United States

6.1.1 Strategic ends and corresponding ways of the US

End: Dominance in cyberspace. The US aims to achieve and maintain cyberspace superiority in both peace and conflict, using cyber operations to secure lasting advantages and enhance its kinetic and informational strengths (USCYBERCOM, 2018; IISS, 2021).

Ways: The US is building capabilities that support and enable the full spectrum of activities in cyberspace. The US conducts diverse operations that enhance national power and support the Joint Force, including persistent campaigning, cyber defense, resilience-building, and strategic planning. (DoD, 2023). It engages in detailed planning and ensures the broad dissemination of comprehensive cyber strategies. As a global leader in space connectivity, the US has effective military cyber operations for intelligence, damage assessment, and targeting. (IISS, 2021) The US also has a leading role in global cyber alliances and communities, having effectively defended its critical infrastructure and promoted shared security principles. Successful diplomacy, leadership in organizations (e.g., IEEE and ISACA), and contributions to international technical standards strengthen its dominance in cyberspace. (IISS, 2021)

End: Cautious approach of operations. The US aims to manage the risk of unintended escalation and carefully weigh whether to exploit a vulnerability for disruption or preserve access for ongoing intelligence collection. (DoD, 2023; Harding, Pusztaszeri and Dickson, 2025).

Ways: The US conducts cyber operations below the level of armed conflicts and to achieve favorable security (DoD, 2023). The US patiently plans and constructs a concept for the operation, maps the target systems, and waits for third-party approval, but does not proceed further until an opportunity presents itself (Harding, Pusztaszeri and Dickson, 2025).

End: Strong alliances and partners. The US views its global alliances as a core strategic advantage in cyberspace (DoD, 2023).

Ways: The US strengthens ties with cyber-capable allies at the strategic, operational, and tactical levels, integrating these efforts into broader security cooperation (DoD, 2023). Collaboration with NATO, Pacific allies, and Five Eyes partners enhances US cyber operations through joint incident response, shared attribution, and coordinated actions against malicious actors (IISS, 2021; Harding, Pusztaszeri and Dickson, 2025). Through 'defend forward' operations, the US Cyber Command disrupts adversary activities in coordination with allies.

The US builds allied cyber capacity by sharing infrastructure, conducting joint training, providing specialized capabilities, and identifying partner network vulnerabilities to enhance collective cybersecurity and readiness. (DoD, 2023) It leads initiatives (e.g., Cyber Deterrence Initiative), building coalitions to deter malicious cyber activity through shared intelligence, joint attribution, public support, and collective penalties. (Nye, 2010). The US adopts a unified cybersecurity approach, integrating government, industry, academia, state authorities, defense, the National Guard, and privacy advocates (IISS, 2021). The private sector is a vital role in analyzing threats and protecting national infrastructure (Harding, Pusztaszeri and Dickson, 2025).

End: Deterrence building. Cyberspace operations are essential to US military power, supporting integrated deterrence by delivering informational and strategic advantages (DoD, 2023).

Ways: The US conducts cyberspace campaigns that integrate cyber operations with other intelligence disciplines to gather threat intelligence. It uses cyber espionage to monitor leadership decisions, tactical planning, and foreign governments, while also deploying cyber tools to disrupt adversary information operations and nuclear programs, including retaliatory strikes on foreign systems and infrastructure. The US uses deterrence through punishment by responding to hostile acts with great force, making such actions costly for adversaries. It also deters through denial by deploying defenses measures that limit attack impact and discourage repetition. (Harding, Pusztaszeri and Dickson, 2025)

End: 'Defend forward' approach. The US follows a proactive strategy known as 'defend forward', which involves disrupting malicious cyber actors before they can launch attacks. The US is committed to defending its national interests in cyberspace by maintaining readiness to protect its citizens, critical infrastructure, and territorial integrity (IISS, 2021; DoD, 2023; Harding, Pusztaszeri and Dickson, 2025). The US leverages cyberspace as a strategic domain to deter aggression, maintain readiness, and win wars (DoD, 2023).

Ways: The US cyber strategy aligns with national objectives and prioritizes resilient defenses built on strong infrastructure, strategic operations, and advanced technologies (Harding, Pusztaszeri and Dickson, 2025). The US enhances its cyber capabilities to support the Joint Force's mission assurance and collaborates with the science and technology community to develop tools that disrupt malicious cyber actors. The US trains its forces to operate in degraded cyber environments and learns from both adversary and internal operations to improve cyber warfare capabilities and risk management. Acknowledging that cyber risks span the entire defense enterprise, the US strengthens cybersecurity culture across defense by educating leaders, integrating training, and investing in a diverse workforce supported by incentives and private-sector collaboration. (DoD, 2023)

End: Integrating cyber operations with military operations. The US integrates cyber operations into military planning to gain strategic and asymmetric advantages.

Ways: The US develops cyberattack capabilities for all operational phases and across command levels, with each military service maintaining cyber units for offensive and defensive missions. These units support combatant commands and conduct offensive cyber operations when directed (Harding, Pusztaszeri and Dickson, 2025). As part of integrated deterrence, cyber operations are embedded in campaign and contingency planning. The US leverages cyberspace's unique characteristics to achieve Joint Force requirements, including cross-domain effects in large-scale combat operations. (DoD, 2023)

6.1.2 Identified means

The US aims for dominance and deterrence in cyberspace through advanced infrastructure, persistent operations, and integrated intelligence. Strategic planning, legal oversight, and decision-support systems guide cautious execution. Alliances are strengthened via joint training, shared infrastructure, and coalition coordination, while private sector collaboration boosts threat analysis and infrastructure defense. Deterrence relies on offensive tools, espionage, and strong defenses. The 'defend forward' approach uses proactive disruption, resilient systems, and a skilled, diverse workforce. Integration with military operations requires specialized cyber units, cross-domain platforms, and campaign planning to support Joint Force missions.

6.2 Russia

6.2.1 Strategic ends and corresponding ways of Russia

End: Dominance in cyberspace. Russia seeks greater cyber dominance as part of its effort to reclaim great power status (Voo and Singh, 2025).

Ways: Russia emphasizes information as a pillar of state power and uses it as a key tool of statecraft, leveraging cyber operations, propaganda, and strategic messaging to assert power, shape domestic narratives, influence

the global order, and revise the European security architecture. It emphasizes a comprehensive approach to controlling and deploying information both domestically and internationally. (Voo and Singh, 2025) Russia views offensive cyber operations as a key means of achieving information dominance across all stages of conflict (Connell and Vogler, 2017).

End: 'Information confrontation' approach. Russia views the internet as a persistent threat and a strategic weapon, treating the information space as a continuous battlefield where cyber and psychological operations advance long-term objectives (Connell and Vogler, 2017; Sherman, 2025). The 'information confrontation' strategy merges cyber and information operations, encompassing espionage, infrastructure attacks, and psychological manipulation (Dickson and Harding, 2025).

Ways: Russia's belief that it is engaged in an information war with the West drives a proactive and defensive strategy focused on controlling domestic narratives and influencing foreign targets (Dickson and Harding, 2025). Information confrontation is regarded as a strategic tool that can substitute for conventional military force under certain conditions. (Dickson and Harding, 2025). Russia's Information Confrontation Doctrine is supported by diverse funding sources (e.g., the Ministry of Defense and other security bodies), which sustain cyber units and offensive cyber operations (Voo and Singh, 2025). Russia is enhancing its tech-savvy information warfare capabilities, leveraging cybercriminal proxies, deepfakes, and generative AI to increase campaign scale and complexity. Most operations target societal and governmental stability rather than military systems. (Voo & Singh, 2025; Dickson & Harding, 2025)

End: Cooperation. Russia cooperates within its cyber ecosystem to enable actions in cyberspace.

Ways: Russia's cyber ecosystem integrates state agencies, cybercriminals, contractors, patriotic hackers, and private military companies (Sherman, 2025). Russia sustains relationships with cybercriminal groups, which it tolerates and exploits under an informal "social contract" requiring them to target foreign entities, avoid interfering with state objectives, and remain responsive to government directives. (Dickson and Harding, 2025; Sherman, 2025). These actors provide services (e.g., DDoS attacks, malware obfuscation, etc.) while generating revenue and cultivating cyber talent for state use (Connell and Vogler, 2017). Russian intelligence agencies recruit hackers and contractors for offensive operations, including espionage, sabotage, and influence campaigns. Cybercriminal tools have also been adapted for state purposes (e.g. NotPetya attack) (Voo and Singh, 2025).

End: Strategic deterrence. Russia is increasingly using offensive cyber operations to support conventional military actions and integrate them into its strategic deterrence (Connell and Vogler, 2017).

Ways: Strategic deterrence involves coordinated forceful and non-forceful measures to prevent adversaries from taking actions that could cause harm (Dickson and Harding, 2025). Russia employs cyber operations, disinformation, and covert influence to intimidate neighboring states and discourage alignment with Western institutions (e.g., NATO and the EU), while asserting regional dominance and countering Western integration (Voo and Singh, 2025). It also uses information and psychological operations to incite fear and instability in adversary populations, staying below the war threshold to avoid retaliation (Dickson and Harding, 2025).

End: Cyber readiness. Russia's cyber operations fall into two types: high-profile actions for plausible deniability and covert campaigns for espionage and future attacks. State actors provide stealth, cybercriminals offer deniability, and IT firms supply expertise and R&D. (Voo and Singh, 2025)

Ways: Russia's strategy combines espionage, disruption, and influence, targeting infrastructure and shaping public perception, while psychological tactics aim to manipulate opinion and distract governments (Lilly and Cheravitch, 2020; Dickson and Harding, 2025). A decentralized network of proxies, hacktivists, and cybercriminals, often linked to intelligence services, enables disinformation and disruptive campaigns, while avoiding direct attribution. Ambiguity is reinforced through inconsistent control of these actors and the use of front organizations to obscure state involvement. (Connell and Vogler, 2017; Lilly and Cheravitch, 2020; Dickson and Harding, 2025) Russia's cyber strength is built on a legacy of Soviet engineering education and a strong talent pool, drawing recruits from both legal and criminal sectors. It is supported by a hybrid culture that merges digital expertise with military strategy. (Connell and Vogler, 2017; Soldatov and Borogan, 2022)

End: Integration of military, cyber, and information operations. Russia considers cyber and information operations central to its military and intelligence strategy (Dickson and Harding, 2025; Sherman, 2025).

Ways: Russia's concept of warfare has evolved to include non-military measures, such as psychological, electronic, and cyber operations, that can be deployed before or without conventional conflict. These

capabilities enable covert influence over infrastructure and populations, blurring the line between peace and war. (Lilly and Cheravitch, 2020; Voo and Singh, 2025) Although Russia stresses defense, its actions indicate an increasing focus on offensive capabilities (Connell and Vogler, 2017).

End: Information influence. Shaping adversary perceptions is central to Russia's strategy.

Ways: Russia ensures regime stability by controlling its domestic information space through censorship, surveillance, infrastructure manipulation, and suppression of dissent, reinforcing narratives of external threats. Technical and psychological tools (e.g., cyber capabilities, legislation, media control, and strategic messaging) are used to suppress opposition, unify public opinion, and counter Western influence. (Voo and Singh, 2025) Russia combines infrastructure control and cognitive manipulation to influence adversary perceptions and decisions (Lilly and Cheravitch, 2020). It conducts global information warfare, especially in Africa, Latin America, and the Middle East, using cyber operations, disinformation, military presence, and covert funding to pursue geopolitical goals. Domestically and abroad, Russia relies on state media, education, historical revisionism, and influence campaigns to dominate the information space. It employs sophisticated narrative manipulation, using contradictory messaging and reflexive control to confuse, destabilize, and steer adversaries toward favorable outcomes. (Voo and Singh, 2025)

6.2.2 Identified means

Russia's pursuit of cyber and information dominance relies on extensive resources, including state institutions and intelligence agencies, a robust cyber talent pool drawn from both legal and criminal sectors, and a legacy of strong technical education. It leverages cybercriminal groups, patriotic hackers, private military companies, and IT firms to provide technical expertise, operational capabilities, and plausible deniability. Advanced tools enhance the sophistication of operations, while state media, educational systems, and legal mechanisms enable control over domestic narratives and global influence campaigns.

6.3 China

6.3.1 Strategic ends and corresponding ways of China

End: Information dominance. China views information dominance as central to modern warfare, enabling effective operations across all domains (air, land, sea, space, cyberspace, and the electromagnetic spectrum).

Ways: Controlling information is considered critical for managing escalation and gaining strategic initiative (Cheng, 2019). China emphasizes denying adversaries access to information domain to achieve operational superiority (Costello and McReynolds, 2018). Its military strategy focuses on targeting enemy networks, command systems, and combat units through information warfare, including influence operations and precision strikes on IT infrastructure (Cheng, 2019). China also seeks to degrade adversary decision-making by disrupting information processing, transmission, and collection through both kinetic and non-kinetic strikes. A key concept is 'information isolation', which involves disabling C4ISR systems to reduce situational awareness and delay responses. (Burke *et al.*, 2020)

End: Paralysis and cognitive dominance. China prioritizes disabling an adversary's systems through targeted paralysis and decapitation rather than outright destruction.

Ways: China aims to "win without fighting" by shaping adversary decisions and achieving objectives below open warfare. This includes, for example, rapidly dominating and resolving conflicts, providing strategic information support, and emphasizing the importance of preemption in information warfare. (Costello and McReynolds, 2018; IISS, 2021) China's 'Three Warfares' strategy encompasses psychological, public opinion, and legal warfare. It regards the cognitive space as a critical battlefield. The strategy seeks to shape narratives, weaken adversaries' resolve, and secure diplomatic and informational advantages through psychological impact, particularly in the early stages of a conflict. (Burke *et al.*, 2020)

End: Cooperation. China's cyber strategy centers on cooperation with military, civilian, and private actors to build a state-supported cyber ecosystem and gain asymmetric advantages.

Ways: Through military-civil fusion, China partners with tech firms to enhance capabilities and global digital influence. It employs contract hackers, state-sponsored groups (e.g., Volt Typhoon), and hacktivists for espionage, infrastructure infiltration, and intellectual property theft, often blurring the lines between state and non-state actors (IISS, 2021; Pusztaszeri, Harding and Dickson, 2025). China's cybersecurity infrastructure includes national research centers and commissions that integrate private sector expertise into military cyber operations (Pusztaszeri, Harding and Dickson, 2025). Internationally, China promotes cyber norms emphasizing

state control, working closely with Russia and SCO members, and supports broader state participation through the OEWG to counter Western influence (IISS, 2021).

End: Active defense. China follows an 'Active Defense' strategy, asserting that it will not initiate cyberattacks but will retaliate if attacked (Cheng, 2019; Pusztaszeri, Harding and Dickson, 2025).

Ways: China focuses on strengthening cyber defenses to ensure resilience and effective response. To protect cyberspace sovereignty, it employs economic, legal, diplomatic, and military tools, including pre-positioned assets for precision "hard kill" attacks such as disabling power grids. (Pusztaszeri, Harding and Dickson, 2025) China's cyber operations prioritize espionage and information exploitation to advance political and economic objectives, including intelligence gathering for strategic advantage, AI development, and cyber readiness. (IISS, 2021; Pusztaszeri, Harding and Dickson, 2025) China integrates espionage with offensive capabilities to enable flexible responses below escalation thresholds, targeting intellectual property, personal data, and critical infrastructure (Costello and McReynolds, 2018; IISS, 2021).

China's cyber strategy aligns with national goals. It combines targeted and opportunistic attacks and includes malware and disinformation cooperation with Russia (Pusztaszeri, Harding and Dickson, 2025). China emphasizes speed and precision, accelerating the reconnaissance-control-attack-evaluation cycle, with PLA commanders acting on timely intelligence (Burke *et al.*, 2020). Advanced C4ISR technologies support information superiority in joint operations. (Pusztaszeri, Harding and Dickson, 2025). China aims to reduce dependence on foreign technology and lead in core internet technologies through initiatives (e.g., Made in China 2025 and the Digital Silk Road), promoting Chinese infrastructure and standards globally. It shapes global standards in emerging technologies (e.g., IoT, IPv6), pursues AI leadership, and develops space and cyber forces to strengthen cyber power. (Cheng, 2019; IISS, 2021; Pusztaszeri, Harding and Dickson, 2025)

End: Integrating cyber and military operations. China is modernizing the PLA to conduct informatized operations under its "systems destruction warfare" strategy (Burke *et al.*, 2020).

Ways: The "systems destruction warfare" strategy supports political objectives by gaining information dominance, expanding strategic reach, and dismantling adversary systems (Burke *et al.*, 2020). The PLA prioritizes real-time data sharing, precision strikes, and intelligent munitions to enable low-collateral, integrated warfare across physical and informational domains. Early operations focus on shaping the battlespace through intelligence and non-kinetic actions, delaying strikes until information superiority is achieved. Joint operations integrate all service branches through networked, digitized systems, breaking hierarchies and synchronizing efforts across levels, with emphasis on cyber, electromagnetic, and space domains. (Burke *et al.*, 2020; IISS, 2021)

End: Control and censorship system. China regards cyberspace as a domain with weak international norms, asserting sovereignty over its own internet while exploiting access to others. This asymmetry legitimizes censorship, media manipulation, and cyberattacks (including on civilian infrastructure), as strategic tools. (Pusztaszeri, Harding and Dickson, 2025)

Ways: Domestically, China prioritizes thought control and suppression of Western ideologies to maintain stability, which it considers essential for national development and public well-being. Foreign cyber interference (e.g., political disruption or data theft) is considered a major threat to internal security and personal data protection. (Pusztaszeri, Harding and Dickson, 2025) China operates the world's most advanced cyber surveillance and censorship system. The Great Firewall restricts foreign content and limits external access to Chinese platforms, reinforcing information dominance and shaping public perception. Information warfare combines content restrictions with economic and cyber pressure to deter foreign influence. The Ministry of Public Security manages domestic surveillance and cybersecurity. It conducts inspections, accesses user data, and evaluates system vulnerabilities, impacting nearly all foreign firms and strengthening state control over corporate and personal information. (Pusztaszeri, Harding and Dickson, 2025) China's laws require foreign firms to store data locally, increasing state control. China's cyber governance model influences other authoritarian states (e.g., Vietnam and Russia), which are adopting similar internet regulations. Additionally, China exports surveillance technologies (e.g., facial and voice recognition and smart city systems) that enable mass data collection and AI-driven monitoring. (IISS, 2021)

6.3.2 Identified means

China invests in advanced C4ISR systems, AI tools, and space-based ISR platforms to achieve information dominance. For paralysis and cognitive dominance, it needs psychological warfare teams and information-

influence capabilities. China builds cooperation through partnerships with tech firms, national research centers, state-sponsored hackers, and international alliances. Its active defense strategy involves robust cyber defenses, pre-positioned strike assets, and intelligence systems. Integration of cyber and military operations requires modernized PLA units, networked command systems, intelligent munitions, and space-cyber forces. The control and censorship system relies on the Great Firewall, AI-driven surveillance technologies, strict data localization laws, Ministry of Public Security infrastructure, and exportable monitoring tools to reinforce domestic control and influence abroad.

7. Discussion and Conclusion

Cyber superpowers share similar high-level strategic goals related to dominance, approach, cooperation, and integration. They also pursue goals concerning defense, deterrence, influence, readiness, and control, which vary by nation. Although nations may share similar strategic goals, the measures taken to achieve them differ, as the US, Russia, and China pursue cyber power through distinct strategic approaches.

The US emphasizes defense, deterrence, and cooperation, integrating cyber capabilities into conventional military planning and global alliances. It maintains a cautious, rules-based approach. Russia adopts a confrontational and disruptive model, viewing cyberspace as a battlefield for psychological and informational warfare. It leverages a decentralized ecosystem of proxies and cybercriminals to achieve strategic objectives, often targeting societal stability and public perception. China aims for comprehensive information dominance, integrating cyber operations deeply into military modernization and global influence campaigns. Its strategy combines state control, technological development, and cognitive warfare, with the goal of shaping both domestic and international narratives.

This paper has several limitations. The material used in the analysis consists of Western literature, which may introduce a cultural or geopolitical bias in the analysis and interpretation. Additionally, due to language constraints, the authors relied on literature available in languages they could understand, potentially excluding relevant works published in other languages. Future research could address a broader range of original documents and adopt a more systematic approach to selecting source material. Expanding the review to include source material from countries known for their advanced cyber capabilities would provide a more diverse perspective on the topic.

AI declaration: AI tools were not used in the creation of this paper.

Ethics declaration: An ethics declaration was not required for the research.

References

Braun, V. and Clarke, V. (2012) "Thematic analysis," in H. Cooper, P.M. Camic, D.L. Long, A.T. Panter, D. Rindskopf, and K.J. Sher (eds.) *APA handbook of research methods in psychology*. American Psychological Association (Research designs: Quantitative, qualitative, neuropsychological, and biological, 2), pp. 57–71. Available at: https://doi.org/10.1037/13620-004.

Burke, E.J., Gunness, K., Cooper, C.A.I. and Cozad, M. (2020) *People's Liberation Army Operational Concepts*. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RRA394-1.html (Accessed: November 10, 2025).

Cheng, D. (2019) *Testimony before U.S.–China Economic and Security Review Commission*. Heritage Foundation. Available at: https://www.uscc.gov/sites/default/files/Cheng_USCC%20Testimony_FINAL.pdf (Accessed: November 10, 2025).

Connell, M. and Vogler, S. (2017) *Russia's Approach to Cyber Warfare*. Center for Naval Analyses.

Costello, J. and McReynolds, J. (2018) "China's Strategic Support Force: A Force for a New Era." National Defense University Press Washington, D.C. Available at: https://digitalcommons.ndu.edu/china-strategic-perspectives/6.

Dickson, J. and Harding, E. (2025) *A Playbook for Winning the Cyber War, Part 2: Evaluating Russia's Cyber Strategy*. Center for Strategic and International Studies (CSIS). Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-09/250903_Dickson_Playbook_Russia.pdf?VersionId=6RPe2gNRM05DWfEZqmvcyyukhE28aVbk (Accessed: November 11, 2025).

DoD (2023) "2023 DOD Cyber Strategy Summary." U.S. Department of Defense. Available at: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf (Accessed: November 9, 2025).

Giles, K. (2021) "Russian information warfare," in T. Clack and R. Johnson (eds.) *The World Information War*. 1st ed. Abingdon: Routledge, pp. 139–161. Available at: https://doi.org/10.4324/9781003046905-12.

Giles, K. and Ii, W.H. (2013) "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, IEEE, pp. 1–17.

Haizler, O. (2017) "The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking," *Cyber, Intelligence, and Security*, 1(1), pp. 31–45.

Hakala, J. and Melnychuk, J. (2021) *Russia's Strategy in Cyberspace*. Riga: NATO Strategic Communications Centre of Excellence. Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/Nato-Cyber-Report_15-06-2021.pdf?zoom=page-fit (Accessed: October 22, 2025).

Harding, E., Pusztaszeri, A. and Dickson, J. (2025) "A Playbook for Winning the Cyber War: Part 5: Evaluating U.S. Cyber Strategy." Available at: https://www.csis.org/analysis/playbook-winning-cyber-war-part-5-evaluating-us-cyber-strategy (Accessed: November 9, 2025).

IISS (2021) *Cyber Capabilities and National Power: A Net Assessment*. International Institute for Strategic Studies. Available at: https://www.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/ (Accessed: October 25, 2025).

Kuehl, D. (2009) "From Cyberspace to Cyberpower: Defining the Problem," in F.D. Kramer, S.H. Starr, and L.K. Wentz (eds.) *Cyberpower and National Security*. University of Nebraska Press, pp. 24–42. Available at: https://doi.org/10.2307/j.ctt1djmhj1.

Lalu, P. and Puistola, J. (2015) *Hybridisodankäynnin käsitteestä*. Research review 1/2015. Riihimäki: Puolustusvoimien tutkimuslaitos.

Lehto, M. and Limnéll, J. (2017) "Kybersodankaynnin kehityksesta ja tulevaisuudesta," *Tiede ja ase*.

Lilly, B. and Cheravitch, J. (2020) "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in *2020 12th International Conference on Cyber Conflict (CyCon)*. *2020 12th International Conference on Cyber Conflict (CyCon)*, Estonia: IEEE, pp. 129–155.

Limnéll, J. (2013) "Offensive cyber capabilities are needed because of deterrence," in J. Rantapelkonen and M. Salminen (eds.) *The fog of cyber defence*. National Defence University/Department of Leadership and Military Pedagogy (2), pp. 200–207.

Lonergan, E. and Montgomery, M. (2021) "What is the Future of Cyber Deterrence?," *SAIS Review of International Affairs*, 41(2), pp. 61–73.

Lykke, A.F. (1989) "Defining military strategy," *Military Review*, 69(5), pp. 2–8.

Mulvaney, D.B.S. (2025) *PLA Views on the Information Domain*. China Aerospace Studies Institute.

Nye, J. (2010) *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. Available at: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/cyber-power.pdf (Accessed: October 25, 2025).

Pijpers, P. and Arnold, K. (2025) "Rethinking Cyber Deterrence: Adapting to the Realities of the Digital Battlefield," *Journal of Strategic Security*, 18(1), pp. 61–76.

Pusztaszeri, A., Harding, E. and Dickson, J. (2025) *A Playbook for Winning the Cyber War, Part 3: Evaluating China's Cyber Strategy*. A Report of the CSIS Intelligence, National Security, and Technology Program. Center for Strategic and International Studies (CSIS). Available at: https://www.csis.org/analysis/playbook-winning-cyber-war-part-3-evaluating-chinas-cyber-strategy (Accessed: October 11, 2025).

Scott, J. (2014) *A Matter of Record: Documentary Sources in Social Research*. John Wiley & Sons.

Sherman, J. (2025) *Confronting Russia's cyber power: reassessing assumptions, sizing up the threat, and building a proactive response*. Washington, DC: Atlantic Council.

Soldatov, A. and Borogan, I. (2022) *Unpacking the Kremlin's Capabilities*. Center for European Policy Analysis. Available at: https://cepa.org/wp-content/uploads/2022/09/Unpacking-Russian-Cyber-Operations-9.2.22-1.pdf (Accessed: November 10, 2025).

US DoD (2010) "Joint Terminology for Cyberspace Operations." US Department of Defense.

US DoD (2021) "DOD Dictionary of Military and Associated Terms." Department of Defense.

USCYBERCOM (2018) "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command." The US Cyber Command. Available at: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf (Accessed: November 9, 2025).

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D. and Schwarzenbach, A. (2020) *Reconceptualizing Cyber Power*. Harvard Kennedy School Belfer Center for Science and International Affairs. Available at: https://www.belfercenter.org/publication/reconceptualizing-cyber-power (Accessed: October 1, 2025).

Voo, J. and Singh, V.V. (2025) *Russia's Information Confrontation Doctrine in Practice (2014–Present): Intent, Evolution and Implications*. The International Institute for Strategic Studies.