Technical Means, Strategic Ends: Cyber Deterrence Challenges in the Context of China and Russia's Information Warfare Doctrines

Sam Paulson

Graduate Student at Johns Hopkins
School of Advanced International Studies
IW SWG FAN

The views expressed in this article are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of Defense, or the U.S. Government.

Introduction

This paper explores the complex interplay between cyber operations and broader information warfare strategies, illustrated by the doctrines and operations employed by Russia and China. It argues nations use cyber operations as tactical tools to achieve specific information warfare objectives as aligned with their doctrines. This paper applies both established and emerging deterrence and coercion studies to cyberspace, outlining the challenges these measures encounter in deterring operations within both the cyber operations realm and the broader information environment. In doing so, it builds upon existing discussions to offer insights and a set of recommendations for navigating the complexities of information warfare.

Understanding Russian and Chinese Perspectives of Information Warfare

Russia

Russia uses information warfare to destabilize economic, social and political systems of its targets through psychological influence, altering the target's decision-making process to better suit Russia's goals (Thomas 2015, 12). The importance of information to Russia's strategy is underscored by the Kremlin's belief that the West is trying to influence the thinking of Russian citizens, believing "there is a real cognitive war underway in the ether and media for the hearts and minds of its citizens," per a NATO analysis (Thomas 2015, 12). While the West typically views war and peace as binary states, focusing more on kinetic conflicts, Russia perceives itself to be in an ongoing information confrontation with the West (Hakala and Melnychuk 2021, 34).

Russia wages information warfare by continuously engaging in information operations to create divisiveness within the West, sow discord and diminish the U.S.'s global perception and influence in world affairs (Jones 2018, 2), all while staying below the threshold of triggering kinetic conflict. Russia has adapted its traditional military deception tactics to the digital domain, using information to weaponize principles such as freedom of speech. These tactics include *active measures*, *reflexive control* and *maskirovka*. Active measures attempt to disrupt the target nation's policies by way of covert action. Reflexive control seeks to force a target to act in a specific manner, often against its own interest. Lastly, maskirovka uses deception to mislead a target into believing in something which does not exist, thus disrupting the target's perception of reality (Hakala and Melnychuk 2021, 11).

China

China views modern warfare as a battle for information dominance which can be achieved through information operations. By dominating the information environment, it aims to control the battlefield, air and sea during combat. China distinctly defines the process of

manipulating information as information warfare, while psychological warfare is defined by how a target receives and interprets manipulated information. (Beauchamp-Mustafaga 2023, 8). Psychological warfare is one of the Three Warfares doctrine; the other two being public opinion and legal warfare (Beauchamp-Mustafaga 2023, 9). Public opinion warfare focuses on tactics such as propaganda and is thus more akin to influence operations, while legal warfare focuses on degrading a target's position by maneuvering within an established legal framework (Beauchamp-Mustafaga 2023, 9). The RAND Corporation's report, *Chinese Next-Generation Psychological Warfare*, further details extensive sub-topics within China's information warfare strategy, indicating China's deep commitment to mastering the information environment.

China employs information to achieve three main goals: to create a global image that is favorable to China, to incentivize foreign countries to engage with China economically and to deter other nations from contesting China on sensitive issues, such as human rights (Turcsányi, Daniel, and Bahenský 2023, 28). In contrast to Russia, who uses information more directly to stoke discord among Western nations and within the U.S., China deploys information operations more subtly and strategically to positively reframe perceptions of China's image on the global stage. For instance, China allocates billions of dollars each year to craft targeted propaganda aimed at international audiences (U.S. Department of State 2023, 8) disseminating this content through print, digital, and social media platforms in 142 countries and in 12 different languages (U.S. Department of State 2023, 10).

The U.S. is Vulnerable to Information Warfare

The U.S. and other nations with democratic and capitalistic economies are particularly vulnerable. For example, research shows users of Meta are more likely to believe false information if it aligns with their existing beliefs (Allcott and Gentzkow 2017, 213). Additionally, Meta's algorithms limit users' intake of counter-attitudinal content which leads to more polarization (Levy 2021, 834). This polarization not only keeps users engaged longer, boosting ad revenue, but it also creates an environment ripe for exploitation by adversaries who exacerbate discord by disseminating false or polarizing information through fake accounts. Since these activities contribute to profitability, a key metric for shareholders, there is a significant lack of incentive to counter them, coupled with the serious implications for freedom of speech that come with attempts to curtail them.

Other vulnerabilities exist within the information environment due to the extensive digitization of its public and private sectors, where sensitive digital records are prime targets for cyberattacks aimed at extracting and leaking information. Such leaks can severely disrupt political landscapes and lead to strategic losses, amplified significantly by the U.S. media's extensive coverage. These vulnerabilities are further compounded by America's leadership in

innovation and technology, making it a key target for intellectual property theft – actions that directly threaten its economic prowess and strategic advantages within the global information environment. Additionally, the pervasive use of digital devices and IoT across the U.S. provides potential opportunities for foreign surveillance and monitoring, posing a critical threat in an era where information dominance is a key aspect of global power dynamics.

Where Cyber Operations and Information Warfare Connect

In information warfare, the information environment serves as the theater of operations, while information operations are the maneuvers and tactical engagements propelling the campaign. Information operations strategically manipulate cognitive processes, perceptions and beliefs (Mueller and Grindal 2022, 82). Cyber operations serve as the precision weapons within this framework, enabling the execution of these information operations. Both Russia and China actively utilize these tactics within the information environment to further their strategic information objectives. Therefore, cyber operations should be viewed not merely as isolated technical maneuvering, but as integral elements of broader strategic information warfare doctrines. This perspective highlights the need for a dual-focused strategy – one that simultaneously addresses the technical complexities of cyberattacks, which target machines, and the information operations that target the mind.

For example, in the 2016 U.S. presidential election, state-sponsored Russian hackers reportedly conducted cyber operations, leading to the theft and subsequent exposure of information from the Democratic National Committee, according to the Mueller Report (R. Mueller 2019). This operation, along with the strategic use of social media accounts by Russia's Internet Research Agency, was orchestrated to incite political turmoil and shape public perception, specifically by undermining confidence in the electoral process and swaying public opinion. By stealing and strategically releasing targeted information, these cyber operations demonstrated Russia's effective integration of cyber capabilities to fulfill its information warfare objectives. This tactic exploits U.S. principles like freedom of speech to manipulate decision-making in ways that serve Russia's goals, such as interfering in political processes.

Literature often concentrates on countering the technical aspects of cyber operations, without analyzing the strategic information warfare doctrines underpinning them. For example, analyzing cyber operations merely through their technical effects – stolen information, denials of service or installation of malware in critical infrastructure – overlooks the objectives in the information environment. Information theft is not just about data acquisition; it allows an adversary to circumvent R&D costs by reconstructing next-generation military technologies. This capability allows for dominance over air, land, and sea, deterring other nations from contesting territorial claims. This approach is integral to China's information warfare strategy,

which attempts to project a message of strength and reshape global perceptions of China's stature and influence. Similarly, a cyberattack on a military satellite or water treatment system might seem intended to only disrupt services. However, from an information warfare perspective, the attack undermines public confidence in a government's ability to secure critical infrastructure. For instance, a cyber operation that disables a communications satellite not only denies the ability to communicate, but also instills fear and confusion among civilians and impacts military decision-making, as aligned with Russia's information warfare strategy.

By recognizing cyber operations as extensions of state-directed information strategies, more effective countermeasures can go beyond technical mitigation of cyber operations to address the strategic intentions behind these actions. This approach involves not only responding to the immediate impacts of cyberattacks but also proactively engaging in the information environment to counteract the strategic aims they serve – in effect, addressing both the cyber operational symptoms and the underlying condition.

Traditional Coercive Strategies Fail to Counter Cyber Operations

Applying traditional strategies of coercion to address cyber operations is fraught with challenges. Deterrence intends to prevent an adversary from engaging in undesirable action by threatening severe consequences should the adversary cross a clearly established boundary (Schelling 1966, 23). Establishing boundaries and enforcing consequences in cyberspace is challenging because cyberattacks are covert, making boundary crossings difficult to define and detect. The lack of clear international norms further complicates this, leaving nations uncertain about what constitutes a breach, and the low cost and frequency of cyberattacks mean implied boundaries are often tested and breached without repercussions.

While deterrence aims to prevent an aggressor's actions, compellence aims to halt or reverse an action already undertaken by an aggressor by initiating or threatening to inflict significant consequences, continuing to apply pressure until the aggressor changes course (Schelling 1966, 72). While compellence helped to end the Cuban Missile crisis by use of a naval blockade, diplomatic pressures and military mobilization, this was only possible due to positive identification of the aggressor. In cyberspace identifying the perpetrator of malicious code can be a lengthy process, often taking months, if even technically feasible (Nye 2017, 50). This delay in identifying the aggressor weakens the effectiveness of compellence in cyberspace. Moreover, even if an adversary is identified, the decision to retaliate with a cyberweapon risks revealing tactics and techniques, potentially rendering those techniques ineffective for future use.

In compellence strategies, while the victim hopes to persuade the aggressor to stop, the onus for halting the attack ultimately lies with the aggressor (Pape 1992, 430). In contrast, deterrence by denial strategies prevents the aggressor from achieving their objectives by

targeting and neutralizing specific vulnerabilities within their military capability (Pape 1992, 441, 443). However, Pape himself cites several limitations of deterrence by denial, all of which apply to cyberspace. First, denial must be focused on a specific 'territory,' (Pape 1992, 441) a challenging concept in cyberspace where the territory consists of hardware, software, and networks, often virtualized or hosted on cloud servers distributed globally. Secondly, if the target's losses can be restored quickly, denial is less likely to succeed (Pape 1992, 442). In cyberspace, if an aggressor's infrastructure is compromised, it may recover rapidly by way of cloud services, automation tools and resources purchased from the dark web – a process easier and faster than replenishing conventional military assets. Lastly, Pape notes deterrence by denial requires specifically targeting and disrupting the aggressor's vulnerabilities (Pape 1992, 442). However, in cyberspace, vulnerabilities are often concealed, rapidly changing and can be difficult to identify or exploit without revealing one's own capabilities. Additionally, these vulnerabilities might be dispersed across different systems and jurisdictions, complicating efforts to effectively target them without unintended consequences.

These strategies fall short in cyberspace because they focus on countering the delivery mechanism – the cyber operation – not the information operation being fought in the gray zone. This realm of conflict, which is more intense than regular state competition but less severe than armed conflict (Jordan 2020, 5), requires a broader focus beyond mere technical responses to cyber operations. The gray zone lacks clear boundaries, complicating the attribution of cyber operations and the ability of denying them. Cyber operations, the technical manifestations of information operations, exploit these ambiguities to operate with relative impunity. In this environment, conventional tools of influence – such as economic power, cultural influence, political alliances and military strength – prove less effective for the U.S., which has traditionally relied on these overt methods. In contrast, adversaries like Russia and China skillfully navigate the gray zone's uncertainties, using cyber operations to advance their information warfare agendas. This approach allows them to avoid the transparency and accountability that accompany more direct forms of conflict. Furthermore, the blending of military and civilian activities complicates responses, while international legal frameworks on use of force and self-defense, tailored for conventional warfare, fall short against the often non-forceful nature of cyber tactics (Nye 2017, 47). As such, effective strategies must integrate an understanding of both the cyberspace and information environment.

Effectiveness of Proposed Cyber Coercive Strategies

Emerging literature offers new cyber specific suggestions, such as alliance building and defense strengthening. Evidence suggests Russia may moderate cyberattacks on well defended targets, as was the case in Estonia particularly after it became a NATO member and strengthened

its cyber defenses (Gannon, et al. 2024). While enhanced cyber defenses and NATO membership may deter cyber aggression, they do not eliminate the adversarial intent to influence the information environment. This was evident in Estonia where strengthened defenses stopped a Russian cyberattack from achieving its technical effect to make a web page unavailable, following the removal of a Soviet-era monument (Higgins 2022). However, this incident demonstrates that stopping the technical execution of cyber operations does not neutralize the broader strategic efforts to impact the information environment. Even though the immediate technical objective was thwarted, the attempt itself may have residual impacts, continuing to shape public opinion and political discourse about the consequences of removing Soviet monuments. As such, cyber defenses are crucial for protecting digital infrastructure, but they cannot fully shield against the strategic use of cyber operations to manipulate the information environment and shape the narrative. A comprehensive approach that addresses both technical defenses and the manipulation of information is necessary to counter these operations effectively.

Other suggestions, such as entanglement and norm creation, are less focused on the technical aspect of cyber defense. Entanglement occurs when the aggressor and the victim are so interconnected that an attack would immediately result in negative consequences for the aggressor. For example, China may fear attacking a U.S. power grid if it feels the costs of the outage will result in economic repercussions that outweigh the benefits of the attack (Nye 2017, 58). However, as the U.S. and China increasingly decouple their economies due to geopolitical tensions and trade disputes, the interdependence required for entanglement may diminish. Additionally, creating norms in cyberspace may help deter cyberattacks by rendering them socially unacceptable. For example, norms that equate certain cyber actions to taboos can significantly tarnish the aggressor's reputation and diminish its soft power, outweighing any potential benefits from the attack (Nye 2017, 60). While this may stop some aggressors from targeting hospitals or water treatment facilities, others may blatantly disregard these norms, as evidenced by the increasing cases of cyberattacks against critical infrastructure targets. Despite the challenges they face, focusing on these methods is worthy as they aim to influence the broader information environment, affecting how actions are perceived and responded to globally.

Other literature suggests the use of offensive cyber capabilities to achieve deterrence by denial (Borghard and Lonergan 2023, 552) while also achieving effect on the information environment. Deterrence by denial, according to this view, can be achieved by continuous offensive cyber operations to disrupt and deny the aggressor's cyberattack infrastructure, while also influencing the aggressor's view on the operational challenges it will face during such engagements (Borghard and Lonergan 2023, 556). By consistently disrupting the aggressor's infrastructure and capabilities, this strategy aims to alter their decision-making calculus by integrating cyber operations into broader efforts to influence the information environment.

Potential Paths Forward

To effectively counter cyber threats and information warfare, the United States must develop a comprehensive understanding of its adversaries' information warfare strategies while integrating cyber operations within the broader information environment. This strategy could be supported by a robust U.S. strategic doctrine on information strategy, clarifying the specific messages the U.S. intends to project in the information environment. In addition to technical effects such as disrupting adversaries' cyberattack infrastructure, cyber operations could be crafted to deliver impactful informational effects, ensuring alignment with broader strategic objectives. A whole-of-government approach could enhance this strategy, fostering collaboration across the Intelligence Community, the Department of Defense and civilian agencies.

A deeper understanding of adversaries' information strategies could allow the U.S. to strategically exploit vulnerabilities in their information warfare doctrines through cyber operations or other means. For example, given China's focus on positively reshaping its global image, the U.S. could craft counter-narratives that expose discrepancies between China's projected image and its actual policies. By supporting investigations and publicizing credible information on issues like human rights abuses and environmental neglect, the U.S. can undermine China's credibility and diminish the effectiveness of its information campaigns. Intelligence collection and analysis focused on the fusion of cyber operations and information strategies is crucial. This integration will enable more precise identification of adversaries' tactics, intentions and vulnerabilities, vital for producing countermeasures that confront and disrupt both their cyber and information operations.

Collaborating across agencies could help integrate cyber and information operations into a broader information strategy. For example, USCYBERCOM's *persistent engagement* strategy, aimed at degrading adversaries' technical cyber capabilities and strengthening the DoD's internal cybersecurity (U.S. Cyber Command 2022), could be expanded to include operations that impact the information environment and disrupt adversaries' decision-making. Enhanced cooperation between the Intelligence Community and the Department of Defense could provide the expertise needed to achieve this, particularly through units and frameworks focused on influence and information operations, such as ODNI's Foreign Malign Influence Center, DoD psychological operations (PSYOP) units and policies such as the DoD's 2023 *Strategy for Operations in the Information Environment*.

Building on this foundation, a whole-of-government approach can also incorporate elements beyond the traditional defense and intelligence sectors. Engaging law enforcement and existing interagency efforts such as the FBI's Cyber Division, the National Cyber Investigative Joint Task Force (NCIJTF) and the Joint Terrorism Task Forces (JTTF) could enhance the

understanding and integration of cyber operations and information strategies within U.S. borders. Simultaneously, the Department of State could boost the informational impact of these operations by aligning them with U.S. diplomatic efforts, thus ensuring that operations support broader foreign policy goals. Such interagency synchronization not only ensures consistency across all information strategies but also maximizes the impact of U.S. cyber and information operations, ultimately bolstering national security and advancing American interests globally.

In the realm of international norms related to cyberspace and the information environment, the U.S. must take initiatives in forums like those addressing cybercrime, such as UN Resolution 74/247. This resolution, heavily influenced by Russia and China, risks establishing a framework that could potentially pave the way for authoritarian norms (Bannelier 2023). It is crucial for the U.S. and allies to influence these international norms in the image of democratic governance, promoting transparency and accountability, rather than allowing them to reflect the restrictive practices characteristic of authoritarian regimes.

Adopting a 'denial by education' approach, like Finland's strategy of educating school children on identifying false information (Gross 2023), may enhance resilience against information warfare. Integrating media literacy and critical thinking into educational systems and public campaigns can equip citizens to better analyze and resist manipulative tactics on social media employed by adversaries. Implementing this approach could enhance defenses against informational effects, thereby increasing the costs of conducting influence campaigns. This effectively extends the concept of deterrence by denial from the cyber infrastructure realm into the cognitive domain.

Finally, the U.S. should anticipate and prepare for emerging technical challenges and explore how they may affect both cyber operations and the information environment. These include the potential for quantum computing to break current encryption standards, the risks of source code hijacking within open source software to insert backdoors, the concerns over authoritarian governments exporting 5G equipment and the expanding array of low-earth orbit internet satellites which will further intensify the dynamics of the information environment. To better anticipate these challenges, it is crucial that the U.S. engage with the private sector, academia and research institutions to assess their implications at the intersection of cyber operations and information warfare.

Conclusion

To effectively navigate the complexities of cyber threats within the information environment, it is crucial to understand that cyberattacks are more than mere technical disruptions or acts of data theft. Instead, they are often integral components of broader information campaigns that aim to achieve significant geopolitical objectives. In this context,

traditional deterrence models fall short by concentrating solely on the technical aspects of cyber operations and neglecting their strategic informational goals. This paper seeks to contribute to the ongoing discourse by advocating for a reevaluation of cyber operations through the lens of information warfare. It offers suggestions to better integrate these operations within a comprehensive information strategy by leveraging existing capabilities and interagency collaboration.

References

Allcott, Hunt, and Matthew Gentzkow. 2017. "Social Media and Fake News in the 2016 Election." *The Journal of Economic Perspectives , Spring 2017, Vol. 31, No. 2* (American Economic Association).

Bannelier, Karine. 2023. *The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights.* January 31. https://www.lawfaremedia.org/article/the-u.n.-cybercrime-convention-should-not-become-a-tool-for-political-control-or-the-watering-down-of-human-rights.

Beauchamp-Mustafaga, Nathan. 2023. *Chinese Next-Generation Psychological Warfare.* RAND Corporation.

Borghard, Erica D., and Shane D. Lonergan. 2023. "Deterrence by denial in cyberspace." *Journal of Strategic Studies* 46 (3): 534-569.

Braw, Elisabeth. 2022. *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression.* Rowman & Littlefield.

Congressional Research Service. 2023. "Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements." Congressional Research Service.

Gannon, J. Andrés, Erik Gartzke, Jon R. Lindsay, and Peter Schram. 2024. "The shadow of deterrence: Why capable actors engage in contests short of war." *Journal of Conflict Resolution* 68 (2-3): 230-268. https://journals.sagepub.com/doi/full/10.1177/00220027231166345.

Gross, Jenny. 2023. *How Finland Is Teaching a Generation to Spot Misinformation.* January 10. https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html.

Hakala, Janne, and Jazlyn Melnychuk. 2021. *RUSSIA'S STRATEGY IN CYBERSPACE.* NATO Strategic Communications Centre of Excellence.

Higgins, Andrew. 2022. *Estonia says it repelled a major cyberattack claimed by Russian hackers.* August 18. https://www.nytimes.com/2022/08/18/world/europe/estonia-cyber-attack-russia.html.

Jones, Seth G. 2018. "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare." CSIS, October 1.

Jordan, Javier. 2020. "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict." *Journal of Strategic Security* 14 (1): 1-24.

Klimburg, Alexander. 2020. "Mixed Signals: A Flawed Approach to Cyber Deterrence." *Global Politics and Strategy* 62: 107-130.

Levy, Ro'ee. 2021. "Social Media, News Consumption, and Polarization: Evidence from a Field Experiment." *American Economic Review.*

Mueller, Milton, and Karl Grindal. 2022. "Information as Power: Evolving US Military Information Operations and their Implications for Global Internet Governance." *The Cyber Defense Review* 7 (2): 79-98.

Mueller, Robert. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* U.S. Department of Justice.

Nakashima, Ellen. 2022. *Cybercom disrupted Russian and Iranian hackers throughout the midterms.* December 22. https://www.washingtonpost.com/national-security/2022/12/22/cybercom-russia-iran-attacks/.

Nye, Joseph Jr. S. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44-71.

Pape, Robert A., Jr. 1992. "Coercion and military strategy: Why denial works." (The Journal of Strategic Studies) 15 (4): 423-475.

Schelling, Thomas. 1966. *Arms and Influence.* Yale University Press.

Sherman, Justin. 2022. *Russia's Internet Censor is Also a Surveillance Machine.* September 28. https://www.cfr.org/blog/russias-internet-censor-also-surveillance-machine.

Thomas, Timothy. 2015. " Russia's 21st century information war: working to undermine and destabilize populations." NATO.

Turcsányi, Richard Q., Jan Daniel,, and Vojtěch Bahenský. 2023. *Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries.* Riga, Latvia: NATO Strategic Communications Centre of Excellence.

U.S. Cyber Command. 2022. *CYBER 101 - Defend Forward and Persistent Engagement.* Oct. 25. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

U.S. Department of State. 2023. *How the People's Republic of China Seeks to Reshape the Global Information Environment.* U.S. Department of State Global Engagement Center.