THE FUTURE OF CYBER COMPETITION

Annotated Bibliography

September 12 & 13, 2023

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Annotated Bibliography

The Future of Cyber Competition

Prepared By: Samuel Hickey, Thomas Van Bibber, Brandon Williams, Cherry Wu

Panel Topics:

1. Lessons from Ukraine for Peer Adversaries
2. Lessons from Ukraine for US & Allied Cyber Strategy
3. The Nexus of Cyber and Information Competition
4. The Nexus of Cyber and Technology Competition
5. The Prospects for Public-Private Partnerships & National Cyber Readiness
6. The Prospects for Improved Integration

Panel 1: Lessons from Ukraine for Peer Adversaries

- What cyber lessons are China and Russia learning from the war in Ukraine?
- What cyber lessons will other adversaries and competitors draw from Ukraine?
- How will these lessons drive adversary and competitor war planning and kinetic operations?

Landau, Susan. "Cyberwar in Ukraine: What You See is Not What You Get." *Lawfare*, September 30, 2022. https://www.lawfaremedia.org/article/cyberwar-ukraine-what-you-see-not-whats-really-there.

> Given Russia's extensive history of using Ukraine as a cyber testbed, strategists widely expected cyberattacks to be centerstage throughout Russia's war in Ukraine. However, as Landau argues, Russian cyber strategy in Ukraine has more closely resembled harassment rather than warfare, but not because Russia lacks the technological or tactical sophistication for conducting destructive cyberattacks. Ukraine's cyber defense was bolstered by unprecedented levels of cooperation between U.S. intelligence agencies and American tech companies that limited Russian cyber operations. Russia's struggle integrating cyberattacks and kinetic operations shows how cyberwarfare alone remains unsuitable for conquering and occupying territory. Characterizing the domain as irrelevant ignores ongoing Russian cyber-enabled information warfare that seeks to destabilize the West. Dedicated public-private cyber cooperation will be critical for combating Russian information warfare.

Takagi, Koichiro. "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine." *War on the Rocks*, July 22, 2022. https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/.

> Chinese military doctrine is innovating to encompass cognitive warfare—using technology to fight an enemy's biology, brains, and emotions—with the PLA's latest strategy of AI-enabled intelligentized warfare emphasizing human cognition as the lifeblood of warfighting. Chinese strategists are learning from Russia's inability to dominate the psychological battlefield in Ukraine. The PLA will continue investing in cyber tools for cognitive warfare, but they will also strive to improve coordination between kinetic capabilities and cyber tools for cognitive effects. In addition to locating weaknesses in Chinese psychological strategies, the United States and allies should construct their own counter-conceptions of cognitive warfare and integrate them throughout their existing physical warfighting operations.

Vićić, Jelena and Rupal N. Mehta. "Why Russian Cyber Dogs Have Mostly Failed to Bark." *War on the Rocks*, March 14, 2022. https://warontherocks.com/2022/03/why-cyber-dogs-have-mostly-failed-to-bark/.

> Russia has surprisingly forgone large-scale cyber operations in Ukraine, perhaps deterred by Ukrainian cybersecurity cooperation with the United States or senior military leaders simply were unconvinced of cyberwarfare's battlefield relevance. Regardless, the authors

maintain that the West should continue practicing offensive restraint in cyberspace. Sophisticated Stuxnet-style attacks offer limited signaling effectiveness and risk unwanted miscalculation and escalation, even across domains. Cyber-enabled information operations may demonstrate more value by targeting the morale of Russia's military and general populace. This approach would counter Russia's own information campaigns and magnify political pressure on Putin, without the danger of open escalation.

Wilde, Gavin. "Cyber Operations in Ukraine: Russia's Unmet Expectations." Carnegie Endowment for International Peace, December 12, 2022. https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

Wilde contends that Russia's unmet expectations in cyberspace are likely attributed to the relative inexperience integrating offensive cyber operations with kinetic warfighting strategy. The Russian bureaucratic structure also locates cyber authorities in agencies dedicated to intelligence, not combined-arms warfare. Significant tactical stumbles in the war's early stages likely eroded leadership's confidence in the strategic value of cyber operations. Critical to appraising the performance of Russian cyber operations in Ukraine is understanding Moscow's expansive and nebulous approach to information warfare. Russian information warfare doctrine blurs the distinctions between technological and psychological targets, foreign and domestic threats, and peacetime and wartime.

Panel 2: Lessons from Ukraine for US & Allied Cyber Strategy

- What successes can the US and allies point to in coordinating responses to Russian cyber operations?
- Where can improvements be made within existing organizations and processes?
- What regulatory or legal changes should the US and allies adopt to improve interoperability and build norms?

Gady, Franz-Stefan. "6 Wrong Lessons for Taiwan from the War in Ukraine." *Foreign Policy*, November 2, 2022. https://foreignpolicy.com/2022/11/02/lessons-ukraine-russia-war-taiwan-china-military-weapons-strategy-tactics/.

National security decision makers should exercise caution when applying lessons from the Ukraine War to future conflict planning for Taiwan, as many lessons learned remain highly contingent on Ukraine's unique circumstances. Initial conclusions on the sparse effect of cyber operations should not be loosely applied to Taiwan. Limited Russian activity should neither downplay the strategic potential of offensive cyberwarfare nor overstate the resilience of digital infrastructure against future cyberattacks. For example, the utility of commercial space technologies like Starlink or Amazon cloud services for cyber defense could significantly diminish in conflicts directly involving the United States. Ground stations, servers, satellites, and factories would become targets for long-range precision strikes.

Kirsch, Svenja and Bethan Saunders. "Addressing Russian and Chinese Cyber Threats: A Transatlantic Perspective on Threats to Ukraine and Beyond." Paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2023. https://www.belfercenter.org/publication/addressing-russian-and-chinese-cyber-threats-transatlantic-perspective-threats-ukraine.

> Cyberattacks pose a pernicious threat to transatlantic democratic institutions, essential infrastructure, and economic stability. The authors illustrate why the robust U.S.-European Union partnership is uniquely poised to meet this challenge by addressing Russia's current cyber threats throughout Europe and the strategic dangers presented by China's increasingly sophisticated cyber capabilities. The United States and European Union should leverage this moment of unparalleled unity against Russian aggression to make lasting improvements in collective cyber resilience. Such transatlantic efforts to combat disinformation, cement industry support, enhance intelligence sharing, and strengthen digital governance will pay dividends towards preventing cyberwarfare in the coming decades.

Kramer, Franklin and Barry Pavel. "NATO Priorities: Initial Lessons from the Russia-Ukraine War." Atlantic Council, June 13, 2022. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-priorities-initial-lessons-from-the-russia-ukraine-war/.

> The war in Ukraine has cemented key operational priorities for maintaining NATO's deterrence and defense capabilities in the post-invasion security environment. To thwart future cyberattacks, cyber infrastructure supporting NATO mission assurance should incorporate zero-trust architectures, advanced threat hunting, and continuous vulnerability analysis. Such efforts must be strengthened and supplemented by unprecedented levels of coordination with the private sector to secure non-governmental critical infrastructure. NATO's warfighting capabilities relies on private sector networks, and planners must heed lessons from public-private cooperation during the Russia-Ukraine War to ensure resilience.

Krebs, Chris. "Real War Trumps Cyberwar." *Foreign Policy*, January 5, 2023. https://foreignpolicy.com/2023/01/05/russia-ukraine-next-war-lessons-china-taiwan-strategy-technology-deterrence/#chris-krebs.

> Krebs maintains that pre-invasion efforts to boost Ukrainian cyber-resiliency likely deserves considerable credit for thwarting Russian cyberattacks. U.S. Cyber Command, NATO, and industry organizations partnered with Ukraine's cyber defenders to remediate vulnerable networks exposed by prewar network infiltration and post-invasion disruptive Russian cyberattacks. The strategic success of these hardening measures showcases the value of preparation and prevention in the cyber domain. Krebs concludes that it also demonstrates the cyberwarfare remains a contributing factor—not a decisive one—in deterring violence.

Panel 3: The Nexus of Cyber and Information Competition

- What lessons can democracies draw from the intersection of cyber and information campaigns waged during the Ukraine War?
- How can cyber diplomacy build norms and reduce volatility to safeguard a free and open internet?
- What is the appropriate division of labor between the US and allies in this space?

DiResta, Renee and John Perrino. "U.S. Influence Operations: The Military's Resurrected Digital Campaign for Hearts and Minds." *Lawfare*, October 11, 2022. https://www.lawfaremedia.org/article/us-influence-operations-militarys-resurrected-digital-campaign-hearts-and-minds.

> In 2008, U.S. Special Operations Command launched the Trans Regional Web Initiative to promote U.S. interests globally through websites and social media. Data from these efforts revealed a cluster of inauthentic accounts to promote pro-U.S. and pro-Western narratives without clear attribution. The authors argue that the use of inauthentic accounts and fake engagement undermines the truthful information campaigns that have been a cornerstone of U.S. information efforts. The United States and its allies should focus on promoting transparency and truth to counter adversarial networks.

Healey, Jason. "Ukrainian Cyber War Confirms the Lesson: Cyber Power Requires Soft Power." Council on Foreign Relations, April 4, 2023. https://www.cfr.org/blog/ukrainian-cyber-war-confirms-lesson-cyber-power-requires-soft-power.

> Healey argues that Ukraine's resilience against cyberattacks can be attributed to its strong connections with allies, global technology firms, and networks of cooperative information security experts that established a well of soft power. He points to the case of Ukraine to demonstrate why soft power is integral to the effective wielding of cyber power. The importance of soft power in cyber defense extends beyond Ukraine, as states seek to build international support in the face of cyber threats from adversaries like Russia and China. The United States should continue to cultivate soft power through rebuilding its alliances and networks to achieve diplomatic and operational success in the cyber domain.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures." Center for Strategic and International Studies, July 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

> Authors of this empirical analysis of cyber operations in Ukraine conclude that cyber's effects will influence strategic outcomes through political warfare and espionage, but not tactical warfighting. Although the authors acknowledge the limits of the Ukraine case study, evidence supports the argument that cyber's battlefield use is limited and instead holds more power for information operations. The U.S. government should prioritize

resilience in formulating policy to defend against Russia's and other nations' cyber-enabled information operations. The Department of State's Global Engagement Center is one venue for cooperating with allies to counter misinformation. Policymakers should appropriate more funds and attention to the vexing issue because the automation of disinformation and misinformation may tip the calculus in favor of malicious actors.

Sheives, Kevin. "How to Support a Globally Connected Counter-Disinformation Network." *War on the Rocks*, January 20, 2022. https://warontherocks.com/2022/01/how-to-support-a-globally-connected-counter-disinformation-network/.

Sheives argues that governments and social media companies have been ineffective in combating the global threat of disinformation, and heavy-handed regulation can lead to censorship and the politicization of truth. Western companies, platforms, foundations, and governments should focus on providing resources and training to local civil society groups. Funding these efforts will require adopting a more flexible and long-term approach. A coordinated and networked response, led by civil society, is essential to safeguard the global information space for democracy and reliable information. Neither states nor technology companies are positioned to fight disinformation. Both are essential for providing actors in civil society with the tools, intelligence, and funding to build a trustworthy global network to contest disinformation.

Panel 4: The Nexus of Cyber and Technology Competition

- How are emerging competitive dynamics changing technology development and diffusion?
- How will technology and technology competition change the cyber domain and its competitive dynamics?
- What advantages will innovation in AI and quantum create (i.e. offense versus defense, first mover versus fast follower, etc.)?

Kilcrease, Emily. "How to Win Friends and Choke China's Chip Supply." *War on the Rocks*, January 6, 2023. https://warontherocks.com/2023/01/how-to-win-friends-and-choke-chinas-chip-supply/.

In the wake of the 2022 export controls targeting China's advanced semiconductor production, supercomputing, and AI sectors. Kilcrease argues that the United States should remain focused on a clear national security justification. Policymakers should help mitigate economic impacts for foreign partners and offer exemptions on extraterritorial dimensions of the new export controls rules if countries were to adopt comparable measures. While aimed at limiting China's technology advancement, these unilateral controls have caused tensions with key partners in Europe and Asia. The challenge lies in building a consensus approach, given divergent views on how aggressively to decouple from China in advanced tech sectors.

Lin, Herb. "A Retrospective Post-Quantum Policy Problem." *Lawfare*, September 14, 2022. https://www.lawfaremedia.org/article/retrospective-post-quantum-policy-problem.

> In May 2022, the White House issued National Security Memorandum 10 outlining solutions for the threat posed by quantum computing to public-key cryptography. While efforts have been made since 1994 to develop cryptographic algorithms resistant to quantum computing, policymakers have not addressed the post-quantum problem with adequate speed. Quantum computers could jeopardize communications, critical infrastructure, and financial transactions without adequate standardization of post-quantum encryption. Today's encrypted messages could be decrypted in a post-quantum world to potentially reveal sensitive information. Policymakers must prepare for this eventuality and assess the potential impact of a data breach in the future when sensitive messages are decrypted.

Lohn, Andrew, Anna Knack, Ant Burke, and Krystal Jackson. "Autonomous Cyber Defense – A Roadmap from Lab to Ops." Center for Security and Emerging Technology, June 2023. https://doi.org/10.51593/2022CA007.

> The authors of this report outline the future of automated cyber defense and indicate that autonomous cyber defense agents will perform better with reinforcement learning. Automated cyber defenders can react at the speed of the opposing attackers, and reinforcement learning can train AI cyber defense to detect, react, and harden faster than human defenders. The promise of this technique requires further research to test its viability. Government, industry, and academia must nurture this field with funding, training environments known as gyms, data, and the human and digital infrastructure to test reinforcement learning.

National Quantum Coordination Office. "Summary of the Workshop on Cybersecurity of Quantum Computing." November 2022. https://www.quantum.gov/wp-content/uploads/2022/11/2022-Workshop-Cybersecurity-Quantum-Computing.pdf.

> The Workshop on Cybersecurity of Quantum Computing determined that immediate action is necessary due to the threat posed by quantum computers to the cryptography underpinning the nation's cybersecurity. Standardizing secure-by-design cybersecurity tools are essential to prepare for a post-quantum future. Delaying research and deployment would leave the United States vulnerable. The Workshop emphasized the need to secure quantum computing systems and algorithms from hacking and unauthorized access from advanced nation-states. Participants stressed the importance of continuous research to keep pace with the development of quantum computers. The workshop identified key research directions for large-scale control systems, distributed quantum computing, identifying attack vectors on various quantum computers, formal methods for secure systems, and verification of security properties in quantum computers.

Panel 5: The Prospects for Public-Private Partnerships & National Cyber Readiness

- What progress has been made in public-private cooperation to overcome past differences?
- Are the coordinating mechanisms for talent and threat intelligence sharing finely tuned, or do they require more investment?
- How can the public sector integrate technologies in a timely fashion?

Google. *Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape*. February 2023. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

> Authors of Google's one-year analysis argue that Ukraine is under near-constant digital attack and Russian government-backed attackers are seeking to gain a wartime advantage in cyberspace. According to the authors from Google's Threat Analysis Group (TAG), Moscow's goals were to undermine the Ukrainian government, fracture international support for Ukraine, and maintain Russian domestic support for the war. The authors assess with high confidence that Russia will continue to wage cyberwar against Ukraine and NATO partners, and TAG expects that disruptive attacks will increase in response to battlefield developments. A year into Russia's invasion of Ukraine, TAG's analysis shows a steady tempo of attacks and information operations that illustrate the importance of collective cyber defense against malicious state actors.

Microsoft. *Defending Ukraine: Early Lessons from the Cyber War*. June 22, 2022. https://aka.ms/June22SpecialReport.

> Microsoft was a key partner for the pre-war and wartime defense of Ukraine's information architecture, and one of the critical lesson from this experience is that countries must prepare to quickly transfer digital operations away from physical facilities into cloud servers to protect vital warfighting infrastructure. The authors conclude that Ukrainian defenses withstood a stream of attacks due to advances in threat intelligence and internet-connected end-point protection. However, Russia's cyber operations are targeting governments, companies, and non-governmental organizations outside Ukraine, and they are launching massive cyber information campaigns to win support for their war effort. The authors conclude it will take a coordinated and comprehensive effort to strengthen global cyber defenses.

Pell, Stephanie. "Private-Sector Cyber Defense in Armed Conflict." *Lawfare*, December 1, 2022. https://www.lawfaremedia.org/article/private-sector-cyber-defense-armed-conflict.

> Pell argues that the private sector's role in defending against Russian cyber operations has matured beyond past assistance in wars. The private sector brings indispensable knowledge and resources that the government has relied upon, but this reliance creates potential pitfalls. She contends that private companies should not compromise consumer privacy to support government efforts. Government actors must also share with industry the zero-day and other vulnerabilities they uncover for offensive cyber operations.

Finally, she insists that the private sector needs to provide evidence in its public forensic reporting, because unsubstantiated claims can undermine global response to cyberattacks.

Smeets, Max. "Building A Cyber Force is Even Harder Than You Thought." *War on the Rocks*, May 12, 2022. https://warontherocks.com/2022/05/building-a-cyber-force-is-even-harder-than-you-thought/.

Smeets breaks down the challenges to establishing an effective cyber command into five categories consisting of people, exploits, toolset, infrastructure, and organizational structure, and he outlines why building a cyber force poses several difficulties. Not only does an aspiring cyber power need technical personnel, but it needs strategists to integrate cyber operations into mission goals, lawyers to ensure operations comply with the laws of war, and communications experts to coordinate with the private sector. To launch effective offensive cyber operations, Smeets suggests that a command structure needs the infrastructure to run the operation and preparatory infrastructure to test the tools before deployment. When thinking through the future of cyber warfare, he notes that more attention should be given to the costs of finding the right expertise to ensure operational success.

Williams, Brandon Kirk. "Biden to Private Sector: Cybersecurity is Your Responsibility—Not the User's." *Bulletin of Atomic Scientists*, May 1, 2023. https://thebulletin.org/2023/05/biden-to-private-sector-cybersecurity-is-your-responsibility-not-the-users/.

Williams argues that the 2023 National Cyber Strategy signals that the nation's status quo for cybersecurity cannot safeguard the United States' cybersecurity in a future of converging technological threats. The private sector's cybersecurity and software products should be based on secure-by-design principles to anticipate vulnerabilities from the internet of things, quantum computing, and the nation's widespread electrification. Business as usual leaves the country susceptible to malicious actors. To remedy this dilemma, the strategy proposes incentives and regulation to write a new cyber social contract. The private sector, not users, bear the responsibility for safeguarding the United States' digital ecosystem.

Panel 6: The Prospects for Improved Integration

- What is the likelihood of integrating cyber into operational military planning?
- What are the expected benefits of improved integration?
- What cyber changes might the US and allies implement to improve conventional and strategic readiness?

Levite, Ariel. "Integrating Cyber into Warfighting: Some Early Takeaways from the Ukraine Conflict." Carnegie Endowment for International Peace, April 18, 2023.

https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544.

> As the world grapples with the cyber lessons the war in Ukraine offers, Levite urges caution in drawing conclusions for warfighting. He argues that there are many characteristics of the conflict that make it unique and not simply transferrable, including Russia's approach to cyberwarfare, the global support for Ukraine prior and during the invasion, and the experience of Ukraine's cyber warriors. Specifically, he notes that the U.S. view of cyber warfare does not align with Russia's conception that ties cyber authorities to its intelligence infrastructure. That institutional and conceptual difference may apply to other non-democratic regimes, which has implications for what different countries believe constitutes an act of war. He asserts that once kinetic hostilities cease, cyber operations may continue to shift the status-quo in Russia's favor.

Lonergan, Erica and Jacquelyn Schneider. "Cyber Challenges for the New National Defense Strategy." *War on the Rocks*, December 17, 2021. https://warontherocks.com/2021/12/cyber-challenges-for-the-new-national-defense-strategy/.

> Lonergan and Schneider examine the challenges and opportunities for cyber in integrated deterrence, noting that the challenges are numerous for practical integration of cyber in national defense strategies. Cyber does not neatly align with tactical and strategic planning. Its utility is greatest when supporting other national instruments of power to provide asymmetric information advantages. For coordinating with allies, despite the difficulties with sharing cyber capabilities, norm development and propagation may provide one of the more productive areas for allied cyber integration. The authors suggest that a cyber strategy of resilience may provide the most benefit for national security and defense integration.

Odgaard, Liselotte. "NATO's China Role: Defending Cyber and Outer Space." *Washington Quarterly* 45, no. 1 (April 2022): 167-183. https://www.tandfonline.com/doi/full/10.1080/0163660X.2022.2059145.

> Odgaard contends that NATO possesses several instruments for resilience against threats from China in cyber and space, and NATO members can unify without much internal friction. China's growing capabilities in space and cyber challenge the alliance. She suggests that NATO should focus its response to threats posed by Russia and China to the global commons of cyber and space and leverage long-standing U.S.-EU cooperation in both domains. Alliance exercises and capacity-building have wide-ranging appeal for members and can prepare national and NATO networks for malicious cyber actors beyond China. NATO cooperation on cyber and space resilience can deter China, Russia, or other nations from achieving information advantages in the event of war. Focusing on space and cyber fits NATO's mission, delivers internal cohesion, and supports the United States without being overly antagonistic to China.

Lonergan, Erica and Michael Poznansky. “Are We Asking Too Much of Cyber?” *War on the Rocks*, May 2, 2023. https://warontherocks.com/2023/05/are-we-asking-too-much-of-cyber/.

> Lonergan and Poznansky illustrate why cyber optimists and skeptics misunderstand its coercive potential, but that cyber weapons are important tools when integrated with complementary instruments of power to shape strategic outcomes. Cyberattacks have limited utility for the already difficult task of coercion. Governments may turn to offensive cyber operations in the absence of better options. Using these tools, however, may undermine resolve and thus signal the weakness of attempted coercion. In sum, more realism about cyberspace may help policymakers integrate cyber tools into their strategies so that they can identify the right mix of exploits for missions to support broader national strategic goals.

Reports from previous CGSR cyber workshops:

2022: Strategy & Statecraft in Cyberspace
https://cgsr.llnl.gov/content/assets/docs/Workshop-Summary-Strategy-and-Statecraft-in-Cyberspace.pdf

2021: U.S. and Allied Cyber Security Cooperation in the Indo-Pacific
https://cgsr.llnl.gov/content/assets/docs/US_and_Allied_Cyber_Security_Cooperation_in_the_Indo-Pacific.pdf

2019: Strategic Competition in Cyberspace: Challenges and Implications
https://cgsr.llnl.gov/content/assets/docs/CGSRCyberWorkshop2019SummaryReport.pdf

2018: Cyberspace, Information Strategy and International Security
https://cgsr.llnl.gov/content/assets/docs/CGSR_Cyber_Workshop_2018_Summary_Report_Final2.pdf

Center for Global Security Research
Lawrence Livermore National Laboratory
P.O. Box 808, L-189 Livermore, California 94551
https://CGSR.llnl.gov

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-TR-853467