THE FUTURE OF CYBER COMPETITION

Workshop Summary

September 12 & 13, 2023

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

The Future of Cyber Competition

Prepared By: Brandon Kirk Williams and Kimberly Peh with
assistance from Ryan Christenson and Lauren Nyquist

On September 12 & 13, 2023, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) hosted a workshop on the future of cyber competition. This event brought together over 50 participants drawn across the policy, military, academic, scientific/technical, and think-tank communities from the United States and a wide spectrum of allied countries. The discussion was guided by the following key questions:

- What are the key lessons from the Ukraine War for U.S. and allied cyber planning, strategy, and capabilities?
- How can the United States and allies heed the lessons from the Ukraine War to cooperate better and collaborate with the private sector in crisis and peacetime?
- What policy steps should the United States and allies undertake to prepare for the cyber domain's rapidly evolving competitive dynamics amid a climate of technology competition?

Key Conclusions

1. As signified by the tempo and depth of the discussion, this workshop was convened at an opportune moment. Enough time has passed for U.S. experts to assess their own cyber efforts in the Ukraine conflict, and to recognize that the support and capabilities of the private sector may not be sustainable in this conflict or repeatable in the next conflict. While the U.S. Government continues to focus on its own capabilities and bureaucracies, there is a renewed push for understanding how to build durable and useable public-private partnerships for prolonged strategic competition and the next crisis or conflict.

2. Cyber operations remain central to both Chinese and Russian planning regarding the conduct of modern war. There is little concrete public information, however, to describe how Russia and China are adapting planning and policy on cyber operations based on lessons from the Ukraine War. Much then depends on analysis of what experts think they are learning or should be learning. In China's case, they are likely observing the decisive role of outside support to Ukraine (largely originating from private tech companies) and the Ukrainian ability to mobilize its indigenous technical workforce. In Russia's case, they are likely questioning the efficacy of a countervalue cyber strategy targeting civilians and infrastructure rather than a counterforce cyber strategy against military forces.

3. Panelists cautioned that Ukraine may be a special case. It may not define the role of cyber in military conflict in a future conflict with Russia or in a conflict with China over Taiwan. The

next authoritarian leader or military official could be more adept in employing cyber operations. Ukraine had unique advantages—a resilient population, a skilled tech workforce, strong partnerships with the foreign tech sector, and a clear case of Russian aggression and brutality—which may not occur in other scenarios.

4. The U.S. Government and its allies learned salient lessons from Ukraine regarding the importance of presence, persistence, and partnerships. Much of what happened in Ukraine was a validation of Cyber Command's strategy of defend forward/persistent engagement, which were controversial when they were initiated but are now validated as the right doctrine and theory for cyber operations. U.S. Hunt Forward teams also provided key assistance to Ukrainian cyber defenders early in the conflict. Cyber support for Ukraine would not have been possible in an earlier conflict when U.S. and allied capabilities, policies, and legislation were lacking. Allies have evidence that a strong defense can be mounted, but this requires a commitment to long-term resilience and a systematic approach to threat hunting. Norms need to be created and shared, and legislation needs to be passed to allow for future operations.

5. There was a clear recognition of the private sector's support for Ukraine in this conflict, a factor which was seen to be decisive and largely unpredicted. Private companies took a proactive role in publicizing and patching Russian malware such as FoxBlade and assisting Ukraine's transition to the cloud in the early stages of the conflict. Sustaining relationships with the private sector across the U.S. government will be critical to healthy public-private partnerships in the future.

6. Policymakers cannot simply hope that the broad-based public-private coalition that materialized for Ukraine would seamlessly reappear. Russia's aggression was a wakeup call for many in industry. Yet, the effort in the private sector was largely spontaneous, reliant on a sense of civic duty or altruism. Many took on tasks independently in their scarce free time to support the effort above and beyond their day jobs. An incredible trove of researchers suddenly became available, and independently coordinated with their private sector counterparts to solve problems. This need for a sense of greater purpose in their work suggests that carrots far more than sticks could be useful incentives for deepening public-private partnerships.

7. The key to public-private partnership is defining the terms of successful collaboration. Some collaborations are largely performative, with both entities advertising partner logos on their websites with no meaningful work. Meaningful and lasting public-private partnerships require clear incentives for both parties, a roadmap to deepen collaboration to overcome anticipated legal, cultural, and logistical challenges, and mutual points of contact skilled at partnership building.

8. Quantum computing and artificial intelligence (AI) are widely viewed as emerging technologies that could change the landscape of cyber competition. Discussions focused on where these technologies are now, absent the hype about potential futures which often cloud the discussion. Both these technologies have come a long way in the last decade, but there are still limitations. Neither are "silver bullets." Each is a double-edged sword offering advantages both for the attacker and the defender. Generative AI and Large Language

Models (LLMs) will confront policymakers with near-term problems that will necessitate strong public-private cooperation. Geostrategic competition is likely to accelerate the pace of tech innovation, perhaps resulting in countries overlooking quantum's negative externalities or relying on false metrics of success or advantage.

9. Participants suggested ways to better prepare the United States for the anticipated future of cyber competition. Some of these suggestions were organizational, reflecting debates about the dual-hat nature of the National Security Agency (NSA)-Cyber Command or the existing bureaucratic coordination within the U.S. Government. Many focused on how to tap into existing cyber talent for future Ukraine-like crises or conflicts in the form of an organized reserve. Several military and civilian organizations are currently focused on this issue and have already created specialized units. There was also a recognized need to create focused cyber reserve units focused on particular contingencies, regions, or sectors, such as attacks against the financial sector in New York or the energy sector in Texas.

10. The workshop touched on the need for further analysis of democratic versus authoritarian models, both in the cyber domain specifically but also as these different governance models apply to public-private sector relationships and directed technological development. Each of these models have strengths and weaknesses regarding their known approaches. This would be a useful topic for further directed research or workshop discussions.

11. One recognized challenge was how best to integrate cyber into wargaming, scenario-based discussions, and tabletop exercises. Even when the right people are in the room for these events, cyber for a variety of understood reasons specific to the domain and the capabilities (the secrecy of programs, the short shelf life of capabilities, etc.) remains difficult both to realistically inject and to effectively estimate the effects in these discussions.

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?

Experts are still trying to understand what cyber lessons China and Russia are gleaning from Ukraine. Few writing exists in either language from leading analytical or strategic publications, but panelists arrived at a set of conclusions regarding the wartime use of cyber by Russia and Ukraine. Cyber use in Ukraine likely confirms assumptions held by China's People's Liberation Army (PLA) and the Chinese Communist Party's (CCP) leaders on leveraging cyber for warfighting. Public and private assistance to Ukraine showcases American power in cyberspace and justifies PLA doctrine to establish information dominance early to control the tempo of escalation and coerce adversaries. Russians, on the other hand, learned the folly of employing a cyber countervalue strategy to win an information war that would sap Ukrainian resistance without conducting the offensive cyber operations necessary to support a counterforce military campaign. The Ukraine War also reminds Beijing, Moscow, and other nations of the U.S. private sector's technological superiority, particularly when combined with Cyber Command's Hunt Forward teams.

The Ukraine War likely validates Chinese expert arguments supporting the weaponization of cyberspace and clarifies cyber threat actors. PLA cyber strategy will likely endure for local or strategic conflicts. Ukraine crystallized three significant vectors of the cyber threat landscape. First, Chinese writings acknowledge the need to bolster network autonomy to prevent cyber cut off operations in the wake of Western accomplishments in blocking Russia's internet connectivity. Second, non-state actors and netizens' responses to Russian cyber predations revealed individuals' influence in preserving continuity of information service. Third, U.S. technology companies could complicate the PLA's ambitions to achieve information dominance in conventional wars. For China, the support of U.S. companies such as Starlink, Google, and Microsoft proves that U.S. industry is an instrument of national power that can be leveraged by Washington to coerce U.S. adversaries.

Strategists and intelligence operators in Russia likely will not abandon decades of strategic thinking that countervalue attacks in the information domain remain capable of annihilating enemy will or deterring influential non-state actors from rallying resources to a cause. Instead of destroying morale, Russia galvanized a Ukrainian resistance and convinced global civilians to support Ukraine's information war. The history of countervalue campaigns runs counter to Russian doctrine that depicts civilian will as a mechanical, linear force. On the tactical and operational level, Russian forces appear to have learned from initial mistakes by embedding cyber operators with frontline combat units. Integrating cyber units with kinetic warfighters is a complex organizational skill that strains personnel, institutional bandwidth, and resources. Over the medium to long-term, the pendulum could swing in Russia's favor. Altering battlefield dynamics hinges on the organizational clarity to integrate cyber with combined arms, a challenging task even in peacetime. Russian senior leaders may struggle to dislodge decades of assumptions on information warfare that will inhibit battlefield or bureaucratic transformations.

Panel 2: Lessons from Ukraine for U.S. & Allied Cyber Strategy

- What successes can the U.S 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 U.S. and allies adopt to improve interoperability and build norms?

The United States and its allies leveraged the strength of coalitions and partnerships to witness successes through the early engagement of Hunt Forward teams, rapid threat intelligence sharing, and collaboration between the government and the private sector. Hunt Forward teams' operations in Ukraine have allowed both nations to study cumulative Russian malware and cyber campaigns. When the conflict began, the rapid declassification of information and malware sharing with Ukraine and allies garnered support for a broad coalition. This public-private coalition was crucial for taking initiative and utilizing the private sector's talents. Private companies had speed, agility, and subject matter expertise, all of which aided in repelling cyber operations. Microsoft's discovery and disclosure of FoxBlade malware in addition to Google's assistance in transferring Ukraine to cloud-based servers bolstered Ukraine's cyber defense early in the conflict. Starlink, too, was critical for the maintenance of communication for both kinetic operations and information campaigns.

These successes highlighted the importance of sustaining and replicating early engagement, transparency, and deliberate collaboration. Examples include the establishment of NSA's Cyber Collaboration Center (CCC) and the private sector-led global initiative Cyber Defense Assistance Collaborative (CDAC). Repeating the cyber defense accomplishments of Ukraine will be difficult due to the many idiosyncratic factors of the Ukraine War. External aid was a key factor in Ukraine's accomplishments. Ukraine received such extensive aid in part because it was the victim of an unprovoked attack and skillfully used its soft power to rally attention and assistance. For this reason, many private sector entities provided aid in their free time and independent of profit considerations. Companies' involvement cannot be guaranteed in the future as stakeholders start to reconsider corporate interests and their safety. Existing partnerships in crises are often ad-hoc, and more hands-on relationship-building is necessary to scale these relationships before a crisis.

A second factor that complicates the replicability of success is authoritarians' use of cyber tools and control over the private sector. Adversaries may not behave similarly or mirror Russia's cyber errors. More broadly, authoritarian governments may have a unique advantage because of their ability to direct the private sector to meet government's needs in conflicts. Democracies' legislative and regulatory constraints, on the other hand, can delay responses. This problem is especially evident in Europe where states may talk themselves out of interventions because of privacy concerns, fears of retaliation, and the tendency to adopt a peacetime mentality. Democratic governments do have some advantages over authoritarian states. Democracies often possess incomparable soft power, speed, agility, and subject matter expertise. Authoritarian control over the private sector may instead impede their ability to work independently and innovate.

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 U.S. and allies in this space?

U.S. and allied cooperation in assisting Ukraine was a marked success for combined cyber and information campaigns. They learned that transparency, coordination, and cyber diplomacy increased cohesion and unity of action across capitals. The United States should not presume, however, that this degree of accord will persist or repeat in the event of a war with China. Diverging interests could drive a wedge between Europe, Asia, and the United States. Strengthening ties with threat intelligence sharing, standard setting, and diplomatic support in international forums is essential to building transatlantic and transpacific cyber bonds. U.S. policymakers must address diverging European and Asian notions on cyber posture and the Chinese threat. Cyber diplomacy offers one ideal route for the United States to deconflict and find a division of labor in future cyber and information campaigns against Russia and China.

The United States' years of investment in cyber diplomacy has paid dividends. Cyber diplomats were the connective tissue between the United States, allies, and the private sector before and during the conflict. Before the war, cyber diplomats galvanized support in allied capitals by coordinating information campaigns to prevent Russian narratives from shaping perception. Casting light on Russian misinformation prevented Russia's combined cyber and information operations from weakening alliance resolve. Cyber diplomats were additionally a valuable conduit to ensure that Ukrainian cyber defenders received support from American companies. In other nations, such as Costa Rica and Albania, the U.S. State Department channeled foreign assistance funds to aid in cyber recovery after malicious actors targeted vulnerable networks. Ukraine was a pivotal moment for the United States, allies, and partners to cooperate diplomatically, but challenges remain. Conflicting interests in the United Nations will require sustained diplomatic coordination to prevent a fracturing of the internet that will assist Russia's and China's aim to argue for cyber sovereignty.

Diverging threat assessments and national interests require sustained diplomacy between allies and the United States in determining a division of labor. The European Union (EU) and its individual member states insist that they must engage openly with China to find solutions for the roots of cyber instability. Even though Cyber Command has explained persistent engagement, Europeans and Asian allies are still uncertain how to develop independent cyber postures. Rhetoric and doctrine in Russian, Chinese, and U.S. cyber strategies increasingly strike a similar offensive chord in some allies' opinion. Some favor a more balanced or neutral sounding path. European concern regarding responsible behavior in cyberspace leads them to reject internet fragmentation and to participate in forums and on platforms accessible to all nations. For example, the EU recoils at suggestions to ban TikTok. They believe stopping Chinese influence begins with frank discussions on systemic issues, not steps such as prohibiting TikTok.

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.)?

Innovation in AI and quantum may soon reconfigure cybersecurity. Cyber is one among many security domains where AI and, potentially, quantum creates first mover advantages in an ever-shifting strategic competition for technology. Each threat possesses different time horizons and policy solutions. This includes, for example, reacting to AI's volatility and planning for quantum's revolutionary potential to destabilize cybersecurity. AI's benefits could flow to cyber defenders as well as malicious actors, and recent concerns about generative AI have yet to manifest into concrete examples of effects. Regardless, public and private cybersecurity professionals must prepare for near-term volatility created by the accelerating pace and scale of AI innovation. Quantum, on the other hand, is a manageable policy and technology problem. Despite the hyperbole surrounding quantum, gradual advances in quantum computing and threat mitigation roadmaps can prevent strategic surprise. For both technologies, nation states and private sectors will steer the competitive dynamics of development and diffusion.

Despite fears, no evidence exists that LLMs and generative AI have unleashed a new era of cyber instability. The pace of AI innovation, however, could upend this assessment. Few attacks in the wild have been documented using malware generation by tools such as Wormgpt and Fraudgpt or harnessing LLMs to author credible phishing emails. For every cyber vulnerability unleashed by AI, defenders may attain a similar technological edge. Cyber defenders could counteract sophisticated offensive cyber operations with automated vulnerability discovery or by using reinforcement learning that several AI firms are testing at gyms. It is simply premature to forecast if defense or offense benefits most from generative AI or LLMs. The tempo of innovation will strain the public sector's ability to respond to AI's accelerating development, and reacting to AI in the coming years will demand a new dimension for public-private partnerships. Legacy firms and startups are entering into the policy and regulatory space, and establishing a mutually beneficial bond will be essential to ready the government and nation for high tides of AI disruption.

The threat posed by quantum computing will not compromise cybersecurity and cryptography soon. The time when a quantum computer can crack today's cryptography—known as Years to Quantum, or Y2Q—will likely occur publicly over the next decade. Timelines vary for when this will occur. No credible authority can accurately predict Y2Q's date. Quantum inspires sensational rhetoric of a quantum apocalypse for cybersecurity, but policy and technology solutions exist for mitigating the threat. Years of research resulted in quantum resistant algorithms for post-quantum cryptography (PQC) to protect a range of data from basic messaging to secure national security communications. Google and IBM are currently adopting post-quantum measures to prepare for a future of quantum computing. Unlike AI, cyber professionals and policymakers can implement solutions for Y2Q without reeling from its consequences, but PQC consistency is key.

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?

The remarkable progress in public-private partnerships during the Ukraine War should not be taken for granted, and defining success and nurturing relationships is critical for maintaining progress. Private sector leaders and their employees' altruistic behavior illustrated the value of closely matched public-private incentives during a crisis. Continued alignment in crisis and war will falter if policymakers avoid allocating time and resources to build healthy relationships. The public sector must achieve full executive buy in, respect the private sector's boundaries even if intractable, and negotiate past barriers that may arise. Future cooperation during war will inevitably require fine tuning coordinating mechanisms such as CCC and NDAC and pushing government to operate at industry's speed of relevance.

The private sector needs the public sector to prioritize clearly defined roles, trust, and communication on shared objectives to forge a durable public-private partnership. While some C-suite executives are inspired by civic duty and national security imperatives, they are also leaders of companies that must overcome legal, cultural, and logistical barriers that could hinder collaboration. Incentivizing technology companies' support with clearly defined objectives set by trusted interlocutors will be critical to overcoming those barriers to replicate the lessons from Ukraine's collective cyber defense. Existing cooperation is fragile. The public sector should not presume that another "rally around the flag" moment will transpire. Nourishing partnerships with meetings outside of government offices can establish a foundation of trust based on personal connection that will be crucial in crises. Personal ties are the glue for enduring cooperation as well as mediating disagreements that will naturally arise. Government's ability to align incentives and creating bonds of trust demands urgent attention to preserve the public-private breakthroughs since 2022.

The public sector must socialize industry's concerns within government and heed lessons from successful public-private partnerships to inaugurate a model for public-private partnerships that is fit for purpose in an era of strategic competition. National laboratories may bridge public-private interests and are a venue for fostering the type of innovation partnerships appealing to the private sector. High risk, high reward research and development undertaken in national labs offers a space for cutting edge companies to test products early. Early use of technology affords the public sector the ability to shape incentives in addition to the products that they can integrate into government tasks. Companies then can market those products to domestic and global customers, thereby serving national interest overall. The government and national labs may struggle to bridge the gaps uniformly. Irreconcilable cultural differences could prevent certain private companies from initiating partnerships. Another key dilemma stems from the private sector's pace of innovation and product security. Government representatives cannot and should not marginalize security priorities for hardware, software, and research integrity in a heated technology competition.

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 U.S. and allies implement to improve conventional and strategic readiness?

Integrating cyber into operational military planning is challenging but necessary work to prepare for a future cyber saturated battlefield. The U.S. Department of Defense's focus on injecting cyber into campaigning shows promise and reveals the multiple dimensions of integration. At the macro scale, cyber integration can be understood through the deployment of cyber capabilities to reinforce instruments of power. Cyber is a team sport that integrates the tempo of planning among combatant commands in addition to allies and partners' capabilities. At the campaign level, marrying cyber to operational capabilities aims to advance the domain beyond an offense/defense binary way of thinking that hinders the joint force. Finally, combining cyber with multi domain operations for cyber use in war rather than for cyber war is essential for missions where the whole must be greater than the sum of the parts. Integrating cyber capabilities within the joint force will strengthen the Department of Defense's cyber resilience and ability to recalibrate after learning lessons from cumulative cyber competition.

While the United States has initiated steps to integrate cyber into operational military planning, three challenges are on the horizon. First, the United States must take steps to determine how to best integrate cyber during peacetime for future warfighting and intelligence competition. The distinction between warfighting and intelligence influences the demands that will be placed on cyber and how the bureaucracy should be organized to meet the challenge. Second, due to long operational time scales, lags arise between operations and outcomes. Such lags can affect how senior leaders understand operational effects. Third, cyber exists beyond physical space and outside traditional warfighter tools. Integration at this level can be difficult especially when the Department of Defense learns as an enterprise about technological challenges and capabilities required to fulfill missions.

Ukraine demonstrated why allied interoperability is crucial. Hunt Forward teams are one of the best tools for cyber cooperation with allies, and future missions can place trained operators virtually and physically in the operating environment to study adversary methods and malware. Not all allies possess relevant capacities and have potentially divergent economic interests. Some allied countries, for example, may be less willing to oppose Chinese cyber espionage or reject cheap information infrastructure sold by China. These problems are difficult to overcome as partners and allies cannot be coerced to share the same interests, but work can be accomplished to improve allies' capabilities and reduce attack surfaces.

Lastly, professional military education (PME) can also better instruct students on cyber threats and introduce them to war games utilizing cyber. Currently, PME offers limited cyber courses. Officers need training to emphasize cyber integration and more time playing war games that highlight realistic cyber use. This experience would teach a rising generation of officers a baseline of cyber fluency and the value of cyber integration for campaigning.

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-MI-855146