STRATEGY AND STATECRAFT IN CYBERSPACE

Workshop Summary

May 17-18, 2022

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

STRATEGY AND STATECRAFT IN CYBERSPACE

Center for Global Security Research
Livermore, California, May 17-18, 2022

Prepared by Brandon Kirk Williams with contributions from Charlotte Henderson and Lindsay Rand [1]

On May 17-18, 2022, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) hosted a workshop titled "Strategy and Statecraft in Cyberspace." The workshop evaluated the current state of cyber competition and the policies necessary to compete by best unifying the U.S. government, the private sector, and allies. The Ukraine War is testing hypotheses on cyber policy and the role of cyber for integrated deterrence, and analyses in the months since the war began illustrated the value of coordination and anticipatory resilience. Panels focused on the threats in cyberspace emerging from near peer competitors and ransomware gangs, the health of the public-private partnership, cyber coordination with allies, and the role of cyber in integrated deterrence.

The workshop highlighted: 1) Near peer competitors are determined to compete with the United States and allies in the global information ecosystem, and cyber occupies a preeminent place in the toolkit to achieve advantage in information competition; 2) The cyber war in Ukraine demonstrated that anticipatory resilience and persistence prevented a technologically sophisticated Russia from overmatching Ukraine, and institutional innovation at Cyber Command and the Department of Homeland Security attained agility and response objectives; and, 3) Although obstacles exist, public-private coordination and U.S.-allied cooperation before and during the Ukraine War charts a course for strategic competition against near peer adversaries and combating criminal actors such as ransomware gangs that will target U.S. and allies' networks for decades to come.

Discussion was guided by the following key questions:

- How are Russia and China updating cyber-related doctrine and institutions to evolve with changes in the domain?
- What threats in the domain require urgent attention, and what solutions are required?
- How can the U.S., Allies, and the private sector manage complexity in cyberspace to prepare for an era of strategic competition with two near peer adversaries?

[1] The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

Key take-aways:

1. The cyber strategies and doctrines of Russia and China continue to evolve, in part in response to perceived U.S. threats. Both frame their strategies in terms of the competition for advantage in what Russia calls "the information sphere." This is not information warfare as the U.S. has historically understood it. It is a much broader "information confrontation" strategy that seeks to gain strategic advantage by influencing individuals and public consciousness. It involves both offense and defense in a zero-sum competition with the U.S.. Information confrontation aims at controlling content, connectivity, and cognition, combining attacks on the adversary with steps to protect the sovereignty and integrity of their own information spheres.

2. Russia has of course proceeded from strategy development to aggressive operations. While cyber means are a tool for the covert manipulation of the information sphere, Russia appears to have no particular qualms about the discovery of its operations. It does not hesitate to re-attack after discovery. It also conducts false flag operations to reinforce the misimpression that cyber operations cannot be attributed.

3. China has re-focused and reformed its approaches in recent years in reaction to what it sees as U.S. efforts to build coalitions to contain China's actions in cyberspace and to attack its cyber sovereignty with Defend Forward activities. China has put its emphasis on technical self-reliance, on splintering US-led coalitions, and on learning from U.S. activities.

4. A key emerging threat in the cyber domain is ransomware. Reported incidents increased by 85 percent in 2021. Incidents are becoming more sophisticated—using exfiltrated data to add a new point of extortive leverage or attacking at especially vulnerable moments (e.g., attacking hospitals at peak COVID surge). They are also generating larger payouts. Ransomware as a Service (RaaS) is an emerging form of illicit business involving software developers, affiliates to execute operations, and occasionally state sponsors or benefactors. Reporting has linked Russia and North Korea to RaaS, less so China.

5. The response to RaaS must be "all hands on deck." No one actor or institution can address this challenge on its own. A task force approach is needed to define and implement a campaign of activities to deter, defend, detect, and respond. This must be intelligence driven.

6. As a cyber competitor, the U.S. does not mirror the information confrontation strategies of its adversaries. It does not seek to control content, connectivity, and cognition; instead, it focuses primarily on safeguarding connectivity—that is, on ensuring the integrity of data transmission. Over the last decade, the U.S. has set out and refined its basic strategic approach. The Obama administration put down the first markers and defined lanes in the road. The Trump administration granted new authorities and some room for experimentation. CYBERCOM innovated. The Cyberspace Solarium Commission then took stock and charted a new course. The challenges now are to sustain momentum, enhance capacity, strengthen partnerships, and develop metrics to monitor and assess progress and to guide implementation.

7. As a cyber competitor, the U.S. has both strengths and weaknesses. Its strengths include a robust market-driven communications sector and world-class technical innovation, strong public-private sector partnerships, strong alliances, a free press, and a strong instinct to respond if attacked. Its weaknesses include elements of mistrust in those public-private sector partnerships, sometimes competing allied interests, poor allocation of human capital resources, and an information technology base in government that is generations behind. A weakness of a different kind is the propensity to signal intent in cyberspace with declaratory policy; such signals are largely ineffectual, relative to the signaling value of behaviors that de facto demonstrate which malicious cyber activities are acceptable and which are not.

8. As cyber competitors to the U.S., China and Russia are headed in opposite directions. China is well on its way to becoming a cyber superpower, while Russia is experiencing a major brain drain. But both struggle with meeting domestic demands for cyber expertise. By one estimate, 95 percent of cyber job postings in China went unfilled last year. Further, neither China nor Russia has allies upon which it can count to advance their interests; instead, they rely on coercion and bribery to gain influence.

9. In mapping the cyber ecosystem, the role of independent firms should not be neglected. They bring both technologies and expertise to the ecosystem, as well as a capacity for consequential actions, for both good and ill, in the interstate system. Microsoft's role vis-à-vis the Russian war against Ukraine is illustrative. In anticipation of Russian cyber attacks, last autumn it assisted Ukraine in strengthening its defenses. It has reported Russian direct actions by its advanced persistent threat (APT) actors and assisted Ukraine in responding.

10. To improve the competitiveness of the U.S. and its allies in the information sphere, public-private sector partnerships must be strengthened. Over the last decade there has been important progress in this regard but also many challenges and hard lessons learned. The progress is marked primarily by the policy framework first set out a decade ago and subsequent fine-tuning. The challenges came with the Snowden revelations (and the need to build a more solid foundation of trust for public-private partnership) as well as the revelations about Russian interference in the U.S. electoral process (and the need to better protect US political institutions and processes). The effort to rebuild trust has focused on creating new structures of cooperation. More can be done to develop private sector capacity to engage in these partnerships.

11. Improved competitiveness also requires that U.S.-allied partnerships be strengthened. The US has three types of allied partnerships in cyber space: enduring partners (those who have supported the US in wartime), transactional partners (those with whom shared interests are more limited), and opportunistic partners (those involved in protecting specific events, such as the Olympics). These partnerships lend themselves to different purposes: to gain influence, to gain access, to gain insight, to gain the capacity for operational maneuver. Hunt Forward activities provide the opportunity to develop allied

capacities and integrate information and planning for joint operations. Those joint operations range in sophistication from combined to cooperative to integrated.

12. To compete effectively in cyberspace requires the effective management of complexity. Over the past decade, the U.S. and its allies have gotten better at this. But they still aren't good enough or as good as they might be. Doing better requires first and foremost a better common picture of the information sphere ecosystem. This is a shared task and the most useful knowledge will be the knowledge built together. While all allies have something useful to contribute, an outsized responsibility falls on the U.S., which has a breadth of vision that all others lack and a capacity for scalable responses.

13. The Biden administration's focus on integrated deterrence provides an opportunity to advance U.S. cyber security strategy. In the military realm, this focus should accelerate the needed improvements to multi-domain planning and operations without which U.S. actions will lack the needed coherence. The cultural and bureaucratic barriers to such improvements have proven robust. The role of cyber operations in a multi-domain campaign should be to obfuscate, disrupt, and impose costs—but not to replace conventional military operations.

14. But integration is not the solution to the most pressing problems in cyberspace. This is in part because cyber operations are weak contributors to the objectives of deterrence, given their perishable and uncertain benefits. And this is in part because cyber operations must span the entire spectrum of conflict—from peacetime through crisis to war. Along this spectrum, deterrence is not always the primary objective, and the needed forms of partnering for success in cyberspace vary. Cyber Command might sometimes be the supporting command and other times the supported command. For peacetime competition, the U.S.needs coordinated—not integrated—action with allies and partners. This has sometimes proven elusive. The main challenges to such coordination are organizational cultures, leadership priorities, and insufficient trust.

Panel 1: Near Peer Cyber Fitness

- How have Russian and Chinese cyber strategy and doctrine evolved in response to perceived U.S. threats in cyberspace?
- How are Russian and Chinese institutions evolving with changes to perceived U.S. threats emerging from cyberspace?

The United States faces two near peer adversaries that are committed to leveraging vulnerabilities in cyberspace to seek advantage in an ongoing, constant information competition. Russian strategic doctrine nestles cyberspace into its zero-sum information security doctrine to prevent Western intrusions that could undermine sovereignty. Moscow translates this into an active information confrontation against the West where cyber campaigns are a force multiplier for political objectives, such as in the 2016 United States election. Similarly, the Chinese Communist Party (CCP) portrays itself as the victim of a dogged Western cyber-enabled information contest. Starting in 2015, Xi Jinping consolidated party control over cyber in response to shaping events that required bureaucratic innovation to compete in information competition. Lessons from the Ukraine War may convince Moscow and Beijing to accelerate controlling information and data flows, perhaps hastening a global "splinternet" in the decades to come.

Russia's zero-sum mentality emphasizes a constant search for advantage to prevent adversaries from undermining Russia in an information competition. The origin of Russia's cyber strategies can be traced to the 1991 Persian Gulf War that convinced Russian military officials of the centrality of information and information technologies to the future of nation-state rivalry. They invested in technology and human capital to develop a sophisticated force to protect, in Moscow's eyes, Russian digital sovereignty. Russia's parliament enacted a legal regime that enshrined domestic information and digital sovereignty beginning with the Internet Blacklist of 2012. Russia's strategy evolved into a binary of electronic and digital sovereignty that cements state control over the means to spread information. Russia's Federal Security Service (FSB) and Foreign Intelligence Service (SVR) also established sophisticated hacker corps to undermine Europe and the United States. FSB and SVR APTs such as Cozy or Fancy Bear conduct persistent offensive cyber operations to destabilize other states and weaponize information.

China's cyber strategy mirrors Russian information warfare but widens to encompass joint military operations and a search for information overmatch in conflict. Political and technological shaping conditions steered China's cyber institutions to modernize as well as mirror U.S. Cyber Command's doctrine of Defend Forward. Xi's 2015 assertion of party control of the PLA's Strategic Support Force (SSF) ensured cyber campaigns support political objectives. Xi insists that the West's cyber attacks and technology embargoes are engineered to contain China, and this shaping condition has precipitated mammoth state investments in indigenous software, hardware, and the human capital for China's self-sufficiency. The CCP prioritizes technological independence from Western supply chains to deploy cyber and cyber-enabled tools for intelligentized warfare. A primary objective is to ensure that China is not subject to chokepoints that a galvanized United States and its allies would employ to damage the SSF's cyber warfighting capabilities. The CCP is learning in real time from Ukraine, and it would act promptly in future crises to shape perception in a global contest unfolding in the information ecosystem.

Panel 2: Ransomware

- What is the scope and scale of the Russian and Chinese ransomware threat?
- Can Russian and Chinese directed/sponsored ransomware be deterred?
- Are there response options outside of the cyber domain to respond to Russian and Chinese ransomware?

Since the Colonial Pipeline ransomware attack in 2021, the national security implications of a sustained ransomware campaign targeting the U.S. became inescapable. Ransomware mutated in the past decade from a nuisance of targeted harassment to a nation-wide dilemma where targets ranging from schools, hospitals, state and local governments, businesses and critical infrastructure are crippled by RaaS. The scope and scale of the problem requires a whole-of-nation solution that leverages the United States' private and public sectors to prevent ransomware that paralyzes sectors with exorbitant prices to decrypt data. Ransomware attacks are a complex problem that is best managed by a cooperative framework that utilizes tools of law enforcement, diplomacy, cyber defense, and the private sector to curtail the ease by which ransomware gangs operate globally. Panelists agreed that the dilemma should be less considered as state-directed, and rather state-ignored or tacitly approved.

Formulating a strategy to combat RaaS demands an examination of the business model and its agents. Cybersecurity firm Sophos' annual survey the State of Ransomware revealed that 37 percent of respondents suffered a ransomware attack in 2020, and the total jumped to 66 percent 2021. The Sophos poll's rise reveals ransomware gangs' aggressiveness that is accompanied by specialization of RaaS into a global business. Ransomware developers generate the exploits and payloads for affiliates, and ransomware families such as Blackcat offer lucrative payments to developers in an international competition for talent. Developers such as Venezuelan Moises Gonzalez, named in a Department of Justice indictment, sell their services for cryptocurrency to pay for the payload in addition to advice on interacting with diverse victim sets. The RaaS model is adaptive with tailored payloads and techniques contingent upon the target. According to Palo Alto Networks, average ransomware payouts climbed 78 percent to a total of 541,000 in 2021, and in the same year Dark Web forums sharing victim data rose 85 percent. A small number of ransomware gangs recently branched out to extortion to diversify revenue generation. If exposed, ransomware families rebrand but do not cease operations. In other words, ransomware gangs are adapting and professionalizing to improve their operational tempo that deliver higher returns from victims.

Although a large percentage of ransomware attacks originate from Russia, the intersection of ransomware and nation-states occurs with nations as victims, benefiting indirectly, or potentially employing for geopolitical gain. Ransomware outfits such as Blackcat operate transnationally outside of direct guidance from Russia, North Korea, or China. Indirect benefits, however, could flow to adversaries who passively endorse harassment or embarrassment of the United States or Europeans. Adversaries may in the future capitalize on the mutable nature of RaaS to seek explicit gains. States could also use ransomware to conceal espionage or pre-conflict network mapping. For now, ransomware represents a law enforcement and diplomatic problem, not a feature of state-to-state relations that necessitates a deterrence strategy.

Panel 3: Public-Private Partnerships in the Shadow of Cyber Competition

- What strategic strengths and weaknesses exist in the private sector for the U.S. and near peer competitors?
- How should the U.S. leverage public-private partnerships to present Russia and China with multiple dilemmas in cyberspace?
- How do we ensure the whole is greater than the sum of the parts?

For the United States and its near peer competitors, competing in cyberspace is shaped by effective employment of public-private partnerships. The war in Ukraine refined U.S. public-private cybersecurity partnerships—narrowing gaps between Washington and Silicon Valley—and Cyber Command and the Department of Homeland Security (DHS) are cooperating with the private sector unlike ever before. Near peer competitors, however, face mounting public-private obstacles that cannot be overlooked. For Russia, a brain drain that commenced with the invasion of Ukraine is coupled with damaging sanctions that will increase reliance on imported technology. The CCP recognizes its cyber vulnerabilities and is experimenting with state largesse and mechanisms of control to overcome systemic workforce shortages and dependence on Western software and hardware. Although no nation can claim dominance in cyberspace, the maturing U.S. public-private partnership is now more equipped to handle rising geopolitical tensions with near peer competitors in the future.

The future for the U.S. cyber public-private partnership entered a new phase in 2022. Cyber Command and DHS' sharing of cyber threat intelligence combined with Shields Up notifications fortified the relationship. Distrust lingers, but the public-private partnership is far removed from the post-Snowden decay. In a novel instance, Microsoft adopted an aggressive posture to defend Ukraine and combat malicious actors in cyberspace. Microsoft's public reporting chronicled the company's active campaign to protect Ukraine's networks, demonstrating both success and a commitment to reduce volatility in cyberspace. Sustaining the progress from early 2022, panelists emphasized, will require communication that is combined with an awareness of where the private sector can assist the U.S. government and where it cannot.

Near peer competitors' horizons are less clear for overlapping and conflicting reasons. The CCP launched well-financed initiatives to remedy workforce and technology dependence. Sites such as the Wuhan-based National Cybersecurity Center recruits the workforce and incubates the technology to flow into China's cyber ecosystem. Likewise, the CCP's military-civil fusion attempts to channel technology, intellectual capital, and talent into the PLA. These policies strive for a dual cyber circulation model to achieve synergies across academia, the public, and private sectors within China to overcome systemic vulnerabilities. Beijing's shrewd policies may, in the long-term, vault China to an equal footing with the United States.

Unlike China, Russia's future is opaque with consequences from the Ukraine War constraining Russian cyber potential in the long-term. According to Russian analysis, approximately 10 percent of Russia's technology workforce will emigrate in 2022. Semiconductor and hardware sanctions will limit the SVR and FSB's capacity to integrate cyber force multipliers from artificial intelligence and quantum computing. Concluding that Russia will fade from cyber prominence is premature. The SVR and FSB are likely to maintain an aggressive cyber espionage campaign that

could include planting malware in critical infrastructure to hold targets at risk in the future. A resilient, technologically enabled cyber defense is the best front for repelling Russian APTs that will likely grow more desperate in the years to come.

Panel 4: Cooperating with Allies for Cyber Competition

- What strategic strengths and weaknesses exist across allies' capabilities?
- How should the U.S. leverage allied capabilities to present Russia and China with multiple dilemmas in cyberspace?
- How do we ensure the whole is greater than the sum of the parts?

Competing against Russia and China in cyberspace requires effective cyber cooperation, and the war in Ukraine confirmed the added value from this collaboration. For U.S. strategic planners, cooperating with allies requires a familiarity with allies' cyber capabilities. A spectrum of relationships exists that spans partnerships of influence, access, insight, and maneuver. Enduring or occasional allies may cut across partnership categories, and the United States must adapt to allies' political boundaries that may inhibit the United States' operational capacity. Many allies' strengths originate in producing technology that feeds into a broader cyber innovation ecosystem that affords the United States a significant advantage. China responds to this strategic imbalance by utilizing coercion and incentives to support Beijing's philosophy of digital sovereignty. Persistent cyber competition with near peer adversaries ultimately demands the United States modernize Cold War alliance models to provide a unified front in competing with China and Russia across cyberspace.

China's and Russia's postures in cyberspace differ, and the divergence between the two near peers calls for unique strategies. Cyber Command's Hunt Forward teams studied Russian malware before the Ukraine War in countries plagued by routine Russian intrusions. The knowledge of the SVR and FSB APTs' tactics, techniques, and procedures and prepositioned cyber teams blunted Russia's offensive cyber capabilities. Prepositioning and persistence resulted in a less dramatic cyber campaign than anticipated, and the lessons learned from Ukraine could present China with multiple dilemmas in cyberspace in the event of a Taiwan contingency. Prompt action and prepositioning in Indo-Pacific allies' networks can constrain SSF cyber attacks that will unfold at machine speed if China invades Taiwan. Communication and cooperation that excelled in Ukraine, panelists agreed, can be replicated in the Indo-Pacific. Ukraine's proof of concept can guide cyber cooperation in the Indo-Pacific if the United States and allies seize the opportunity.

Ensuring the whole is greater than the sum of the parts presents surmountable challenges if both parties invest in policy and technological solutions. Cyber capacity building and operations development emerge as vital first steps to share tools, expertise, infrastructure, and personnel to enable joint planning. Joint operations contribute to how the U.S. and allies learn by operating, with significant experience gains that facilitate effective future missions. Both sides must leverage their unique strengths—for instance the United States' ability to deliver at mass scale—to stymie Russian and Chinese APTs. Unified action during Ukraine illustrated how U.S.-allied commitments can alter an adversary's calculus during crisis, and it is imperative to build on this success to prepare for potential conflict in the Indo-Pacific.

Panel 5: Integrating Cyber into Integrated Deterrence

- Is integration the solution to the most pressing challenges in cyberspace?
- What are the main challenges to integrating cyber with other domains?
- What are the major benefits of increased integration, and how can progress be achieved in integrating cyber with other domains?

Integrated deterrence's framework weaves warfighting capabilities that span domains and theaters, but cyber does not easily collapse into the strategic concept. Cyber access is ephemeral. Adversaries' internal network threat hunting discovers intrusions or patches vulnerabilities. Unlike conventional weapons, cyber tools are covert and face limited ability to deliver effects during conflict that cannot be easily unified with kinetic warfighting in theaters. Cyber fits best into integrated deterrence when Cyber Command coordinates across combatant commands, the government, and the private sector where incentives are aligned for campaigns to accomplish resilience. The anticipatory resilience witnessed in Ukraine is an example of cyber's potential for integration and planning to prepare for attacks occurring in the domain or to study adversaries' tactics, techniques, and procedures. Cyber fits best when complementing, and not substituting for, other instruments of power to deter near pear competitors.

Campaigning shows an ideal route for maximizing Cyber Command's achievements for a strategy of integrated deterrence that unites instruments of power to attain security in the full spectrum of conflict. Cyber campaigning requires coordination, intelligence collection, persistent action, and communication. Through cyber campaigning, the United States can achieve advantage before a conflict by foster uncertainty in adversaries' strategic calculus. Cyber Command is skilled in campaigning as a result of forming Joint Task Force ARES under General Paul Nakasone to disrupt ISIS' networks. Cyber Command leveraged this experience for subsequent operations that evolved into the anticipatory readiness in conjunction with allies to protect Ukraine from Russia's cyber advantages. Competing against technologically sophisticated near peer adversaries demands that the United States and allies cooperate to deny adversary's avenues for attacks or intelligence-collection. Future wartime information operations, as seen in Ukraine, may hinge upon cyber campaigns that are the result of coordination with allies, the services, and the interagency that will capitalize on Cyber Command's record of achievements.

Panelists noted that despite Cyber Command's laudatory initiatives in public-private coordination and intellectual leadership in producing a strategic vision, the Department of Defense struggles on talent management and acquisitions of information technology that are necessary to protect the country. Currently the cyber personnel force is insufficient for the scope and scale of the challenge across the Department. The Department's culture remains suspicious of a non-traditional workforce and it fails to offer clearances to the people it needs urgently. Perhaps most pressing, the Department runs on an aging information technology architecture. Generations-old software and hardware hamstring the capacity to safeguard Department of Defense information networks or conduct offensive cyber operations. These problems are not intractable. Changes in culture and acquisition are feasible, and the Department possesses the authorities to solve its problems securely and with fidelity to protect the nation.

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-836920