LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-822137

U.S. and Allied Cyber Security Cooperation in the Indo-Pacific

B. K. Williams, V. Chinchilla, E. Lisman, A. Tobey, E. Tuomala

April 30, 2021

Disclaimer

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

U.S. AND ALLIED CYBER SECURITY COOPERATION IN THE INDO-PACIFIC

Workshop Summary

March 30, 31 and April 1, 2021

Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

U.S. AND ALLIED CYBER SECURITY COOPERATION IN THE INDO-PACIFIC

Center for Global Security Research
Livermore, California, March 30, 31 and April 1, 2021

Prepared by Brandon Williams with contributions from Veronica Chinchilla, Evan Lisman, Amanda Tobey, Emilyn Tuomala[1]

On March 30, 31 and April 1, 2021, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory (LLNL) hosted a workshop titled "U.S. and Allied Cyber Security Cooperation in the Indo-Pacific." This session brought together participants drawn across the policy, military, and private sector in the United States and among allied countries in Europe and the Indo-Pacific. The workshop evaluated threat perceptions, assessed cyber power in a regional context, and explored opportunities for building capacity and trust with allies, partners, and the private sector. The region's cyber threat landscape is marked by increasing malicious activity, with threats persistent and ever-growing. Grounded by this strategic reality, the workshop advocated for 1) a concerted push into the arena of norm setting from the bottom up, 2) an agreed metric by which to assess progress, and 3) the creation of future lines of collaborative effort for the United States and its allies to ensure an open, interoperable, and secure internet.

Discussion was guided by the following key questions:

- How urgent is the regional cyber threat to the United States and its allies in the Indo-Pacific? What are its main characteristics? How might it evolve over the coming decade?
- What lessons can be drawn from past and present efforts to strengthen cooperation to address this threat?
- What opportunities exist to improve cooperation and what are the barriers to success?

Key take-aways:

1. The cyber threat has grown steadily over the last two decades and will likely grow substantially over the coming decade. China is an increasingly capable and sophisticated cyber adversary, willing to use cyber means to interfere in regional political and economic dynamics to advance China's development goals. North Korea is less capable but nonetheless oftentimes a dangerous surprise. Russia too is a factor in the regional threat environment as are non-state actors and other states. The threat manifests itself primarily in the ongoing exploitation of cyberspace below the threshold of armed conflict. In armed conflict, cyber activities would likely take new and potentially lethal forms.

[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.*

2. Although approaches to cybersecurity of the United States and its allies have converged as they have matured, important differences remain. Shared best practices have become apparent: resilience, defense, hygiene, strong political control, and improved global governance. Differences flow mainly from different priorities. South Korea focuses primarily but unevenly on how to keep pace with a rapidly maturing North Korean threat and is hampered by domestic distrust of some governmental activities. Japan focuses primarily on China's increased assertiveness in cyberspace and ongoing damage to Japanese economic, military, and political interests. The United States takes a more global view but often favors action over consultation. The differences are not substantial enough to block cybersecurity cooperation, but they do impose some limits.

3. Cooperation improves when threat perceptions converge and when the United States exercises thoughtful leadership. It erodes when efforts to promote convergence lapse, when tactical responses take precedence over strategic trust building, and when the United States sets aside the effort to promote cooperation.

4. U.S. leadership is essential, as every U.S. ally faces real restraints and limits in improving cyber security on its own. The United States has an abundance of bureaucratic resources compared to its allies, but it still lacks a clear vision on how to build a collective and collaborative capacity in a domain centered on secrecy and rapid response. Leadership must be built on meaningful engagement and consultation on all these matters and an appropriate modesty about our collective capacity to meet the challenges ahead.

5. Looking to the future of cybersecurity cooperation among the United States and its Indo-Pacific allies, it is easy to identify numerous challenges, usually arising from frictions over threat assessments, desired end-states, doctrine, language, and the different public-private sector relationships in each country. But these challenges also represent opportunities, places where concrete progress can be made and where frictions lend themselves to concerted action. Progress in working one will reinforce progress in working the others. Unity of command may be a bridge too far, near-unity of action is attainable. An achievable goal is to a place where the US and its allies can convey to an adversary that "to beat any one of us, you to have to beat all of us."

6. China's strategy is comprehensive in nature, designed to contest what it perceives a capable, sophisticated, and belligerent cyber adversary in the United States. It begins with defining a central place for cyber in China's development process and military modernization. In the military domain, China pursues improved defenses and the opportunistic pursuit of information dominance. In the economic domain, it prioritizes reduced reliance on externally-sourced technologies and components alongside incentivizing developing countries to purchase Chinese companies' affordable cyber and surveillance products. In the political domain, domestically it pursues deep social control, while internationally it conducts political campaigns to stake its claim to the moral high ground of global governance.

7. The further development of strategic thought about the ends and means of conflict in cyber space and with cyber tools is hostage to the vocabulary and concepts imported from other domains and not yet well tailored for the realities of cyber competition and conflict. This is

most evident in the use of the vocabulary and concepts of nuclear deterrence to try to elaborate a strategy to compete effectively in cyber space and reduce or otherwise manage cyber risks. In a strategy of persistent engagement below the lethal threshold, deterrence concepts have little value and the failure to prevent or adequately respond to events only erodes the perception that deterrence or compellence is possible in this arena. We've learned enough to try to set aside misleading concepts but not enough to have consensus around more useful ones.

8. In the long-term, diplomacy is as important for cyber security as deterrence and defense. Diplomacy determines the realm of the possible for political cooperation and the realm of the necessary for global governance and a global ecosystem supporting U.S. and allied values. It is the means by which best practices are shared, norms constructed, and oversteps identified and acted upon. But the United States must refresh and renew its approaches. In doing so, it should be guided by the ambition for a much more competitive cyber diplomacy.

9. In an inter-allied strategy to enhance cyber security, priority must be given to improved public-private partnerships. Those partnerships are not built on demand-signals from government or private companies; they are built on trust. Trust is gained through dialogue and experience. It is squandered whenever government loses sight of private sector interests. Over the last decade there has been a lot of mutual learning, but stark examples of how singular events (e.g., the Snowden revelations) can quickly destroy this trust.

10. But this is work that cannot be left to cyberwarriors alone. We must approach the cybersecurity challenge in the Indo-Pacific with an understanding that it is inseparable from the broader strategic challenges in the region, from the emerging challenges of multidomain deterrence and regional net assessment, and from the needed collective responses. More must be done to create a more common understanding of those challenges and responses and of the place of cyber in each. Context matters. Words matter. The only way to improve the level of discussion is through cross pollination. Strategic thinkers must leave their comfort zone to learn the distinct challenges in the cyber domain, and cyber experts should find the familiar through study and discussion of the challenges in other domains.

Panel 1: Calibrating the Threat

- What are the main features of the regional cyber threat?
- Are there significant differences of assessment among allies?

The workshop's opening panel established the baselines for the region's cyber threat landscape, principal cyber actors, and the reasoning behind allies' differing threat perceptions. China's sophisticated cyber power towers over all Indo-Pacific competitor nations and is point of origin for much of the region's malicious activities, with a substantial gap between a second place North Korea. Other recognized nation-state sources of advanced persistent threat (APT) actors, primarily Russia and Iran, play marginal roles in the regional cyber balance of power. Do the United States' Indo-Pacific allies thus loudly object to China's cyber coercion? The magnitude of Asia's economic interdependence routing through China prevents Japan and South Korea from publicly rebuking Chinese cyber interference. The United States' Northeast Asian allies and Australia, nevertheless, suffer no delusions about the gravity of the near- and long-term Chinese cyber threat to national security, democratic institutions, economies, and defense readiness.

A holistic assessment of the regional cyber threat begins by tracing the web of cyber incidents emerging from China. One panelist concluded that the Chinese Communist Party uses cyber resources as a force multiplier for its long-term strategic pursuit of dominating the Indo-Pacific across all domains in addition to boosting its domestic surveillance capabilities. Chinese institutions, such as the Strategic Support Force (SSF), operate freely below the threshold of armed conflict in the gray zone. Beijing's gray zone activities include disinformation campaigns, espionage, election interference, and intellectual property (IP) theft via an increasing number of vectors. Chinese threat actors, for instance APT 30, employed a host of tools to gain networks access to member-states of the Association of Southeast Asian Nations (ASEAN). Intelligence gleaned from ASEAN members enabled Beijing's aspiration to monitor its neighbors' government, civilian, and private sector data for the purposes of political manipulation. From the perspective of 2021, the tenor of China's cyber operations in the gray zone remains constant over the years and show no signs of diminution.

Allies concur with the United States on the region's prevailing cyber threat realities. Allies are wary of retribution and thus reluctant to engage in naming and shaming China. Chinese APTs target Japan and South Korea's technology sectors for IP theft, and threat actors routinely meddle in each allies' domestic politics. North Korea's state-sanctioned cyber crime represents a less pressing dilemma for the region, albeit one that all allies and partners encounter. South Korea bears the brunt of Pyongyang's malicious cyber activity. On the whole, the allies are unified behind a common threat perception, with far less certainty on response.

Allies' perception differs on policy prescriptions to the persistent threat emanating primarily from China. Across a spectrum of public and private leaders, answers vary. Economic integration with China restricts Indo-Pacific allies' freedom of latitude to implement an offensive cybersecurity policy. Allies coalesce around appeals for responsible governance of cyberspace in cyber diplomacy at the United Nations. Allies welcome bilateral cooperation to normalize differing strategic vocabularies to anticipate future conflicts that merge cyber and kinetic effects. Establishing a stable cyberspace in Indo-Pacific begins with the United States and allies planning, conducting open dialogue, and cooperating to contest China in cyberspace.

Panel 2: China's Approach to Cyber Competition and Cooperation

- How does China perceive the cyber threat environment and what opportunities does it see to bolster its influence?
- What are China's military and political strategies for meeting the cyber threat landscape?
- What is China's agenda for promoting international cooperation to mitigate these threats or capitalize on opportunities?

The workshop's second panel surveyed the evolution of China's sophisticated cyber power Beijing wields to meet geostrategic ends. CCP leadership perceives itself as targeted by a determined United States that leverages its superior cyber arsenal to challenge China's sovereignty. China's digitization leaves the country vulnerable to attacks on critical infrastructure, espionage, information campaigns, social unrest, and disruption of nuclear command and control. Despite the CCP's catalog of threats, Xi Jinping and senior leaders identify opportunities to bolster national security by investing indigenous development programs to reduce dependence on foreign technology, thereby reducing the attack surfaces often found in imported technology. The Belt and Road Initiative (BRI) sells Chinese communication tools cheaply to foster a global cybersecurity ecosystem that is friendly to China's domestic authoritarian model and boosts China's ability to undertake espionage campaigns.

In recent years, China reorganized its cybersecurity institutions primarily under the Strategic Support Forces (SSF) to support Xi's holistic modernization of security. The reforms aimed to centralize non-domestic surveillance cyber capabilities into the People's Liberation Army (PLA) to anticipate a future of multi-domain conflict. Cyber units, previously spread across commands, experienced conflicting missions. Consolidating cyber ostensibly reduces internal friction to conduct espionage alongside preparing for kinetic fires, achieving information dominance, defending China's military networks. Domestically, the Ministry of State Security carries out its own cyber activities that can overlap or collide with the SSF. Bureaucratic competition between the two camps may produce effects that could hinder the effectiveness of China's APTs.

Beijing sees several opportunities to leverage international cooperation on cybersecurity to mitigate threats to the CCP. China is active in the United Nations' two cyberspace governance forums—the Group of Governmental Experts and the Open-Ended Working Group—where Chinese delegates capitalize on opportunities to alter the norms discourse in ways that might embed notions of cyber sovereignty to preserve state control. Politically, the Chinese dodge, deflect, and reject any responsibility or blame while trying to shed the stereotype of being bad cyber actors. Also in the UN's technical specialized agencies, representatives from China steer standard setting to support a development strategy to spread Chinese national champions' technology. Wedding BRI assistance to efforts that shape the discourse in governance bodies, empower authoritarian governments, and wage information campaigns aspires to create synergy in the CCP's goal to mitigate threats in cyberspace. Cooperating when and where possible results in an uneven implementation that may not garner long-term results. Opportunism's efficacy, however, should not be discounted when the CCP's senior leadership feels besieged by the United States and sees a protracted competition across domains.

Panel 3: Allied Cooperation: Defining the Baseline

- To what extent do allied approaches to cybersecurity converge or diverge?
- What lessons stand out from past efforts to strengthen cooperation among allies?

Allied cyber security cooperation draws on an enduring relationship. The historic bonds of collaboration, however, equally converge and diverge on cybersecurity. Obstacles among the allies can be overcome, and communication channels exist to navigate the differences to create greater commonalities. The United States and its allies in Japan, South Korea, and Australia meet separately for bilateral cybersecurity working groups to train alongside allies, share threat intelligence, improve supply chains for trusted cybersecurity technology vendors, and build capacity with direct consultation with the United States Cyber Command (USCC). Allies' commitment to augmenting cyber defense capabilities, as stated in national security strategies, mirrors the United States' call for investments in cybersecurity. All parties similarly appreciate the Indo-Pacific's changing security dynamics and prioritize cooperation to preventing cyber coercion against democratic states. Allies agree, perhaps most importantly, on safeguarding a core set of values that exist in and beyond cyberspace.

Allies diverge in a number of areas that cannot be overlooked in a rush to compete against China. Fears of economic decoupling between Washington and Beijing represents a particular threat to East Asian allies. Japan and South Korea's economic superstructure is inseparable from China. The close security relationship must be balanced against the possibility of China using coercive tools of economic statecraft. Economic pain can be inflicted if South Korea, for instance, loudly signals a newfound cyber partnership with the United States. The United States must remain highly sensitive to the economic and security baselines, and China recognizes and exploits this fact.

Although the United States may be reaching improved institutional coherence on cybersecurity, allies' governments struggle to achieve the same accord. Fissures in South Korean domestic politics block meaningful progress toward establishing the vital institutions for improving domestic cybersecurity. Likewise, regional states' embrace of cyberspace governance at the UN may conflict with the United States' strategic goals. Northeastern Asian allies eager to reduce cyber threats persuades them to try and make progress at the UN. Allies bordering China do not have the luxury of time. The consequences of waiting for diplomatic cybersecurity solutions outweigh the benefits of finding common ground in the short-term.

Bilateral cooperation shows signs of progress on both sides. USCC conducts Hunt Forward operations with Indo-Pacific allies, and allies improve Persistent Engagement by granting network access. If allies are unwilling to visibly broadcast cooperation or capacity building, it transpires secretly. USCC, the Department of State, and the Department of Homeland Security (DHS) adopt a flexible approach based on allies' tolerance for public display of cyber cooperation. A vibrant consultative machinery of official cybersecurity working groups, capacity building, or the Track 1, 1.5, and 2 Dialogues exists. A key lesson for the United States and its allies, thus far, has been the limited number of roadblocks for cybersecurity cooperation. Moving forward, the opportunity for ramping up collaboration is strong as long as both parties meet to listen and implement policy based on respective priorities.

Panel 4: Lessons from the Transatlantic Community

- How have the United States and its European allies approached cooperation for cyber security?
- What are the different roles of NATO and the European Union?
- Are there lessons relevant to the further strengthening of allied cooperation in the Indo-Pacific?

The Transatlantic relationship illustrates the complexities of cyber security cooperation. The United States, NATO, and the European Union (EU) share common ground based on decades of partnership across issue areas. All parties agree on the necessity of a free, open, and interoperable cyberspace free from authoritarian state control. NATO members declared that collective defense—enshrined in Article 5 of the NATO Status of Forces Agreement—applies in cyberspace. Within NATO, the United States supports NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) and support for cyber missions. Separately from NATO, the United States retains strong bilateral cyber security partnerships with EU member states. USCC conducted Hunt Forward missions in EU nations to glean intelligence on malicious cyber activities.

The EU and the United States, on the other hand, view operations in cyberspace through different lenses. Consensus-oriented parliamentarians in the EU recoil at the United States' offensive posture led by USCC, preferring legal options such as the EU's Cyber Diplomacy Toolbox to combat APTs. Similarly, the EU opts for a regulatory-heavy path since implementing the General Data Protection Regulation (GDPR) in 2018. Sovereignty plays a leading role in EU member-states' priorities, and Brussels looks askance at the United States' doctrine of Persistent Engagement that implements a security-focused prism to manage the cyber threat landscape.

The EU and NATO occupy different cybersecurity lanes. NATO defends military networks facing outward to protect against cyber attacks from abroad. NATO and EU cybersecurity officers communicate in staff-to-staff interactions. The partnership was forged via exercises and exchanges for the EU Computer Emergency Response Team. Cyber equity holders within the EU coordinate with international counterparts on norms, standards, global governance, and cyber crime. Within the EU, member states' concerns shape cyber policy for information and communications technologies, rights, and regulation. Regional sub-blocs of EU members coordinate on cyber defense. EU members have yet, however, to cohere around a uniform purpose to fully tap its cybersecurity potential in the face of unrelenting attacks.

Key lessons emerge from assessing progress in the Transatlantic cybersecurity experience. Europe's foundation for cybersecurity cooperation began in recent years. CCDCOE regularly assists Australia and Japan, and South Korea partners with the EU's Malware Information Sharing Platform. The EU and NATO took the lead on responding to the request for cyber capacity by Indo-Pacific allies. Panelists concluded the United States and Europe must respect that local context triggers country-specific demand signals. The United States can commit to dialogue that will tailor solutions to country-specific needs. Countering APTs may take time. CCDCOE exercises and capacity building missions demonstrated that knowing local context sets a baseline, and one that will be essential for changing the perception of the cyber threat ecosystem and the solutions necessary to confront adversaries in cyberspace.

Panel 5: Implementing Persistent Engagement

- How much progress has been made in developing and implementing joint doctrine?
- How much progress has been made in developing the needed coordination between CYBERCOM and INDOPACOM? With allies?
- What more should and can be done?

Panelists in the fifth panel addressed innovation in cybersecurity doctrine since 2018. There has been no progress in updating joint doctrine since 2018's Joint Publication 3-12 on Cyberspace Operations. Persistent Engagement was developed in a series of policy moves by USCC, the Department of Defense, and Donald Trump's administration. Doctrine creation can be found outside the Joint Chiefs of Staff due to an intellectual investment at USCC to confront the realities of cyberspace. USCC formulated the Persistent Engagement doctrine—the only combatant command to write doctrine—in 2018. Whereas 3-12 uses a traditional understanding of offense and defense, USCC learned from the operational environment that the offense-defense binary does not capture the domain's character. Instead, initiative persistence with a synergy of offense-defense depicts the operational nature of competition in cyberspace. 3-12 underwent a revision process before USCC articulated the concept of initiative persistence.

The DoD must collaborate internally to set a vision for operating in the region. Coordination between USCC and INDOPACOM is maturing. Both commands must determine how they wish to offer cyber security capacity building, assistance, and integration of cyber effects. INDOPAC and USCC must allocate cybersecurity resources according to the host country's wishes, technological capacity, and the United States' strategy. New operational domains of the twenty-first century call for modernizing security assistance by investing the time to tailor security assistance in coordination with allies. Overcoming allies' cybersecurity gaps necessitates iterative physical and virtual consultations. Although this new imperative requires time, it allows INDOPACOM to collaborate with USCC to dial in the correct level of assistance given each country's sensitivity to an assertive presence in cyberspace, a country's appetite for bolstering network defense, or Indo-Pacific allies' decision to fly their own missions in cyberspace. Coordination will reduce friction, including for commanders who struggle to place cyber effects into operational planning alongside kinetic, on-the-shelf capabilities.

Actors within and outside the United States government frequently rely on the terminology of nuclear deterrence when discussing cybersecurity. Cyberspace, as a domain, does not conform to nuclear deterrence's logic when contest is in the gray zone. Adversaries operating in cyberspace cannot be deterred in the traditional sense. A panelist clarified that the logic of nuclear deterrence can apply to cyberspace in the event of war. Day-to-day operations, however, proved that retaining the jargon of nuclear deterrence is counterproductive. Panel 5's panelists agreed that the United States' national security is best served with a whole of government embrace of Persistent Engagement. Incongruity between USCC and the rest of government, primarily in the legislature, prevents necessary authorities and legislation from guaranteeing the USCC can respond effectively to myriad threats in cyberspace.

Panel 6: Strengthening Collective Cyber Defense

- What should and can be done to enhance cooperation among the United States and its allies?
- Are new institutions needed? To do what?
- Is a special form of leadership required? If so, who can provide it?

Enhancing Indo-Pacific allied cooperation is centered on trust, and the past few years have witnessed a decline in the United States' reliability. Without allied trust in the United States' public and private sectors, defending networks grows harder. Guaranteeing a robust partnership with South Korea's vibrant technology sector, by way of example, enables free flow of threat intelligence, access to cutting edge technology, and continuity of allies' supply chains. Restoring trust is a difficult task, yet one can be accomplished by listening to allies in addition to cooperating on data security legislation for trade. An asymmetry exists between U.S. and Indo-Pacific allies' private sectors, none of which possess the market share for a muscular piece of legislation such as the EU's GDPR. Being attuned to a country's core economic interests in negotiations signals that the United States does not waver in its commitment to allies' long-term economic prosperity. The United States will depend on allies' private sectors to push back on China's efforts to shape norms for 5G, cybersecurity, and technology in governance forums.

Overall, panelists praised the existing institutions for rebuilding trust after years of fracture, urging that consultative meetings receive greater attention. Domestically, DHS' Enduring Security Framework working groups and similar institutional arrangements connect the private sector with DHS' homeland mission. Partnering with the private sector to fight domestic and foreign disinformation campaigns may be an endeavor for a new institution, as the crescendo of misinformation surrounding the 2020 presidential election brought into relief. Overall, the public sector may find itself reliant on the private sector to preserve citizens' trust in democracy and its core institutions. Healing the rift between Washington and Silicon Valley took time, and today the lines of communication demonstrate a restoration of respect and trust between the private and public sectors.

The United States government's leadership role cannot supersede the private sector nor should policy makers request the private sector exceed its ambit. Voluntary public-private partnerships, and not private-public partnerships, are a pillar of the United States' innovation because they can function independently. At no point can or should companies be asked to take the lead on defending the United States. Policymakers must respect the private sector's inability go beyond terms of service to clients and customers. Companies need to remain competitive, and the government should not lose sight of the ensuring corporations' ability to maintain global market share. In the event of cyber escalation that could spill over into armed conflict, the government can turn to the private sector for assistance if both sides foreground trust building and preparation for crises. As one panelist remarked during the workshop, there is only one United States that can use its power to preserve an open, interoperable, and secure internet. In an analogous vein, only the United States government sustains and fosters relationships based on trust at home and abroad. Extant domestic institutions and alliances oblige continuing investment, yet they do not require reinvention for the future of great power competition in cyberspace.

Panel 7: Strengthening Cyber Diplomacy

- What are the roles of diplomacy in supporting cyber security?
- How can diplomatic strategies balance cyber competition and cyber security cooperation?

The workshop's penultimate panel stressed a renewal of innovation in diplomatic practice. An active cyber diplomacy holds the promise of restoring stability to cyberspace, and, for the United States, advocating for a free, interoperable, and secure internet globally. State Department retains the bureaucratic competencies and personnel to enact forward-looking cyber diplomacy, but they have much ground to cover on norm construction, capacity building, and affirming that states follow international law in cyberspace. Diplomacy's most substantial roles are protecting an on-line ecosystem where human rights are respected, restoring stability by reducing incentives for states to act maliciously, and demonstrating U.S. leadership in digital rights and emerging technology. Cyber diplomats at the State Department and DHS cooperate with allies on publicly attributing blame for aggressive cyber acts to state-sponsored APTs. State Department is active in the UN's Group of Governmental Experts and Open-Ended Working Group, lobbying for an internet of information freedom rather than information control by states.

Thus far, as one panelist emphasized, the State Department has not yet framed its cyber diplomacy efforts in the realities of the cyber strategic environment. The State Department can make strides in supporting Persistent Engagement by socializing foreign service officers and diplomats, who are the face of diplomacy, to the domain's competitive nature. Shaping international discourse on cybersecurity norms, responsible state behavior, and governance can be best attained by a corps of diplomats who are unified with the United States' cyber doctrine. Norm construction from the bottom up presents the best route to shape global norms. Leveraging agile coalitions of allies to build norms represents a workable solution to adversary intransigence at the UN. Values, by themselves, do not have the power to influence norms against concerted state pressures to assert authoritarian control over the internet.

Competitive allied cyber diplomacy can shape the standards and norms that determine the future of the internet. A competitive cyber diplomacy relies on the State Department's core competency in creating bilateral and multilateral agreements for capacity building, threat intelligence sharing, resilience measures, and to promote best practices in a competitive cyber ecosystem. Diplomats understand countries' strategic and political environments, and the State Department has the capacity to scale Hunt Forward operations. USCC encounters limits in growing Hunt Forward. Collaboration between the State Department and USCC may present the best avenue to consensually operate in other countries' networks to observe malicious actors. The State Department will guide the United States' cyber diplomacy, not USCC, and integrating cyber authorities will create synergies for how the United States can restore stability in cyberspace and safeguard the United States' cybersecurity.

Panel 8: Framing the Main Strategic Choices

- What lessons can be drawn from the workshop's discussion about how to strengthen allied cybersecurity cooperation?

The workshop concluded with a wide-ranging final panel to take stock and summarize the horizons for cooperation in a future defined by multidomain deterrence. Cybersecurity is one instrument of power for the United States, and experts must place it in a quiver of multidomain concerns in a future clouded by kinetic-and non-kinetic effects of emerging technology. Resolving dissonance in the United States' strategic community will improve the ability to compete effectively in the cyber domain. Not all sticking points will be ameliorated. Dwelling on outdated terminology hamstrings progress on developing doctrine or goals. Applying terminology like deterrence to cybersecurity precipitates friction within the United States, among allies, and for adversaries. The use of deterrence for cyberspace could, in the end, distract more than clarify.

A strong sense of urgency pervades the United States' strategy for cyberspace, and coordinating with Japan, Australia, and South Korea can create opportunities to deconflict. Partnering with allies to find common cause will elevate solutions to a chief bilateral concern. What does the United States set among its top aims? Policymakers in Washington must consult with counterparts in Tokyo, Canberra, and Seoul to appreciate their constraints, priorities, and vulnerabilities. Arriving at common language, along with a shared comprehension of doctrine, can hasten operational cohesion for allies. Integrating cyber capacity building with existing lines of effort could represent a necessary first step to building a tailored model of multidomain security assistance where context is prioritized. Consulting now may help senior leaders write their next strategic documents to anticipate a threat environment where attacks may appear from multiple vectors simultaneously. Institutionally, as domestically within the United States, our Indo-Pacific allies are searching for strategic coherence, and cooperation raises awareness for a new generation.

It is in the United States' interests to be strategically predictable and tactically unpredictable. On setting norms, Washington's cooperation with diplomats in the Indo-Pacific will, as one panelist exhorted us to consider, see beyond the Transatlantic viewpoint and into Asia. In the tactical realm, planners in all countries would benefit from a close analysis of studying adversaries' gray zone logic. Placing unity of purpose and action among the United States' and allies' overriding ambitions can reconcile priorities to action. Integration and collaboration with Indo-Pacific allies places the United States in good stead for being strategically predictable and tactically unpredictable. Challenges exist, but the United States can partner with its allies to regain the virtual commanding heights with the assistance of allies to preserve an open, interoperable, and secure internet against a tide of malicious activities that will not abate.

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-822137