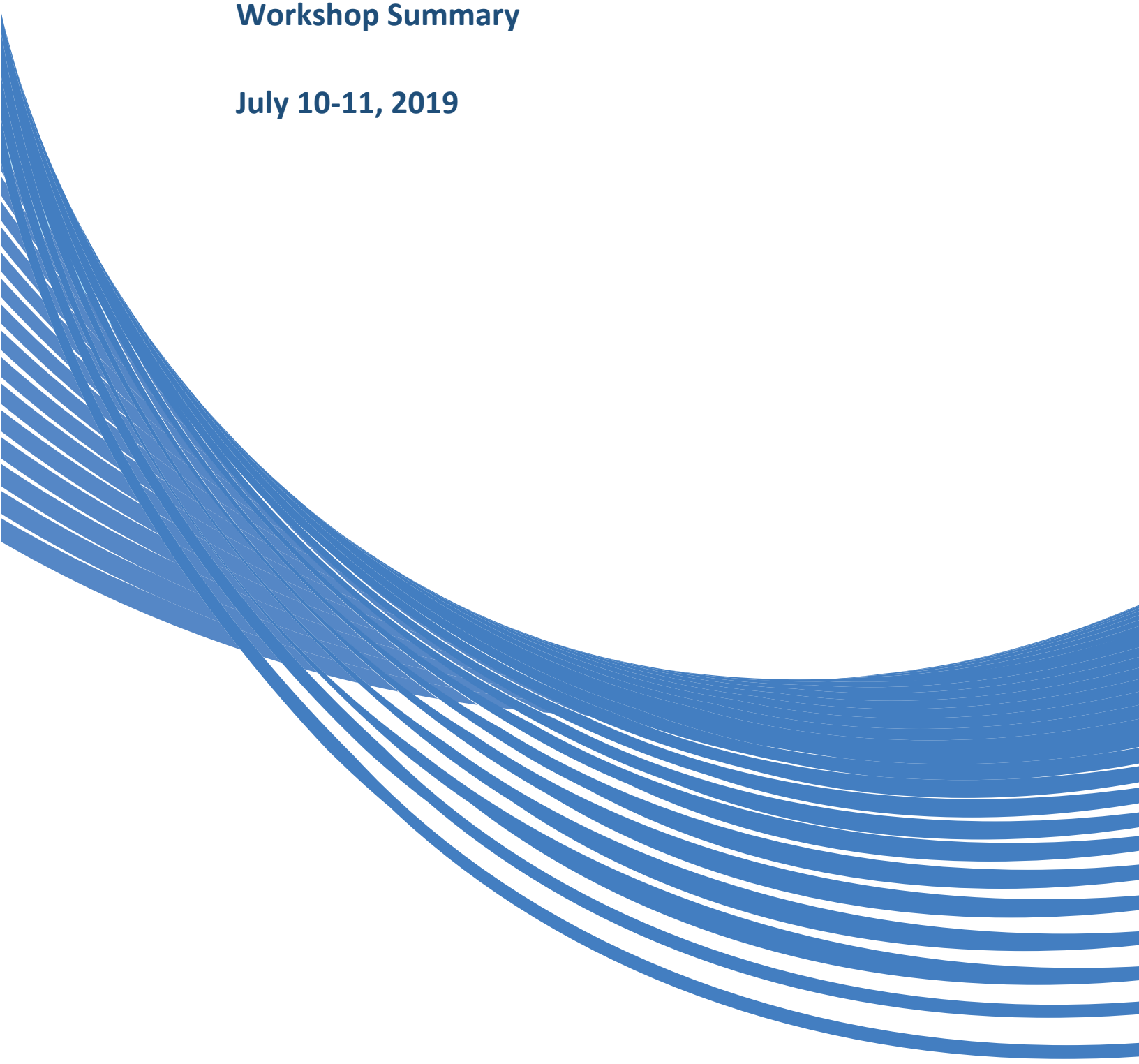
STRATEGIC COMPETITION IN CYBERSPACE: CHALLENGES AND IMPLICATIONS

Workshop Summary

July 10-11, 2019



Center for Global Security Research
LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

Strategic Competition in Cyberspace: Challenges and Implications

Center for Global Security Research, Lawrence Livermore National Laboratory
Livermore, California

July 10-11, 2019

Prepared by Jaclyn Kerr and Alexander Campbell, with Alan Cummings, Anthony Falzarano, Rafael Loss, Scot Purvis, Jacob Sebastian, Justin Sherman, and Jake Tibbetts

The views summarized here are those of the workshop participants and should not be attributed to CGSR, LLNL, LLNS or any other organization.

Key questions:

1. The 2017 National Defense Strategy argues that, in a more competitive security environment, the United States must out-think, out-partner, and out-innovate its adversaries. How does this apply to competition in cyberspace?
2. Administration leaders have set a goal of "over-matching" capabilities and strategic dominance in the technology competition. What does this mean and require in the cyber domain and what risks does it entail?
3. The National Defense Strategy Commission faults the Department of Defense for its so far limited progress in developing operational concepts that link strategy and doctrine to capability development. Are such concepts missing in cyberspace and, if so, what can be done to create them?

Context:

On July 10th and 11th 2019, the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory convened a workshop to examine the nature of strategic competition in cyberspace and the challenges facing current United States cyber domain strategy. The event aimed to situate the discussion of cyber strategy within the broader context of national defense strategy, also taking account of the complex dual-use nature of cyberspace and the variety of stakeholders involved. This was the second workshop that CGSR has hosted on cyber domain strategy and its implications. This event focused specifically on cyber domain military strategy, but with an eye to the implications also for civilian cyberspace, economic and technical interdependence, and democratic Internet governance.

Starting from the 2017 U.S. National Defense Strategy (NDS) and the National Defense Strategy Commission's 2018 critique, the workshop addressed key question about the challenges and risks posed by the current strategic environment, the current state of U.S. strategy, and about how the U.S. can out-think, out-partner, and out-innovate adversaries going forward. The

workshop aimed to contribute to current debates concerning the appropriate roles of persistent engagement, deterrence, and norms in cyber strategy, as well as possible mechanisms for cyber domain risk mitigation. It also sought to understand the perspectives and roles of allies and the private sector in addressing these challenges.

The event deliberately aimed to bridge siloes, bringing together experts from policy, academic, military, and technical communities to engage with and learn from each other in an unclassified not-for-attribution discussion. This included approximately 80 participants from 11 countries, hailing from national laboratories, universities, think tanks, military, government, and the private sector.

Panel 1: Cyber Competition and U.S. Defense Strategy

- Looking back over the last decade or so, what have been the main milestones in defining cyber strategy and integrating it into defense strategy? Is the critique by the NDS Commission sound?
- Looking to the future, what might be the rewards and risks of tripolar competition for strategic dominance? Have we set the right goals and metrics of success?
- What are the necessary roles of cyber diplomacy, in the development of international cybersecurity, Internet, and data policies in support of U.S. national security objectives?

This session reviewed the history of developments in U.S. cyber strategy, its current strengths and weaknesses, and its adequacy for mitigating risks and seizing rewards in an era of renewed great power competition. Participants acknowledged some successes, including the establishment of dedicated institutional structures and some areas of cohesive thought to address particular problems. But significant gaps also were found, including a disconnect between operational and strategic levels, inadequate integration of cyber forces in support of overall defense posture, a lack of conceptual clarity or clear metrics for measurement of success, and an incomplete understanding of cyber-related risks and their mitigation.

Looking back at developments since 9/11, participants acknowledged major progress in reduction of threats to the homeland. Stuxnet was seen as having had significant influence on cyber strategic thought, orienting U.S. strategists around a target-based view (i.e. what targets can be affected through cyber means) and prioritizing the discussion of kinetic effects on targets. This occurred to the exclusion of an objective-based view and produced a focus on protecting critical infrastructure within the United States from cyberattacks with kinetic effects. Defending Department of Defense (DoD) and government networks and deterring cyber adversaries were also emphasized in the 2015 U.S. DoD Cyber Strategy. This approach came to appear inadequate, however, as the U.S. and allies were regularly targeted by adversaries with significant campaigns of cyber aggression below the threshold of armed conflict. These included major data breaches and persistent espionage campaigns, cyber-enabled influence campaigns and election meddling, and intrusions into critical networks—potentially preparing conditions for future attacks.

In this sense, the new 2018 DoD cyber strategy and U.S. Cyber Command Vision represent a significant shift in recent strategic thinking, aiming to "defend forward" through "persistent engagement," operating outside U.S. networks, in "constant contact" with adversaries. The new strategy and corresponding command authorities aim to enable USCYBERCOM to challenge and curtail sub-threshold adversary operations. But there is still significant confusion within the cyber strategy community about the operational implementation of this approach and about its relationship with other elements of strategy, including deterrence and norm development. There is also concern that the focus on "forward defense" against cyber aggression does not adequately address the need to better integrate cyber operations and effects into other areas of defense and warfare—that more work is needed to provide options and capabilities to support the joint force during peace and wartime.

One problem addressed in connection with strategy development was the lack of conceptual clarity and reliance on inappropriate metaphors. Participants pointed out that the U.S. focus on targets and physical effects exemplifies the "logic of war," whereas the "logic of intelligence"—of covert, below-threshold operations achieving strategic effects—could equally be applied to understand strategy and risk in the cyber domain. This might allow clearer understanding of issues like the use of dual-use technologies, the resemblance between espionage and offensive preparations, and the covert or limited-audience nature of many interactions and signals within the domain. Expanding the conceptual lens of cyber operations to draw more on theory of intelligence would not constitute a strategy, however; rarely has intelligence alone achieved strategic effects, while sub-threshold activity in the cyber domain clearly can. Participants also compared the U.S. approach with alternative approaches to cyber strategy of competitor states. China and Russia, for example, both include control over information along with control over technological systems in their cyber strategies. Participants noted these distinct conceptual understandings of the domain itself, though also cautioning against over-generalizing between the two. Some discussed whether the U.S. should engage in a similar integration of information operations into cyber domain strategy, though others were concerned at the repercussions of such mirror imaging by democracies.

Discussion highlighted several risks emerging from tripolar competition for strategic dominance. The lack of a clear shared conceptualization of the domain and the pursuit of contrasting strategies between competing states increases possibilities for misperception and inadvertent escalation. Tripolar competition occurs primarily in the grey zone, and yet the zone's borders remain unclear. It was noted that a goal of "over-matching capabilities" could create escalatory dynamics. Any entanglement between nuclear and cyber issues also remains particularly prone to escalation, with examples discussed including cyberattacks on missile defenses or on nuclear command and control systems. That the prepared capability for such an attack could be known to the attacker alone makes dangerous forms of brinksmanship more likely in crisis situations. Participants broadly agreed that stability should also be a goal of any U.S. cyber strategy, but disagreed over which strategy's operational characteristics best achieved this by limiting vertical and horizontal escalation.

The conversation clarified some differences in perspective among participants about how to assess the current competitive situation—and possibly how to think about measures of success in the future. Participants shared a general agreement that U.S. strategy has yet to adequately curtail unacceptable forms of adversary cyber aggression, and that the successful sub-threshold use of cyber capabilities, in particular, has allowed adversaries to achieve aggregate gains while avoiding direct armed conflict. But different views were presented about how to understand the current preponderance of grey zone conflict. Some focused on the vulnerability of liberal democratic states to grey zone aggression and the success of revisionist adversaries in exploiting their openness to gain substantial strategic advantages. Others held that the location of strategic cyber competition in the grey zone is not a necessary consequence of the technology involved, but an indication of the success of deterrence above the threshold of armed conflict, or of the continuing influence of the liberal, rules-based international order. Cyberspace, they noted, has always been defined by interdependencies and shared rules enabling interoperability, openness, and cooperation despite its frequent mischaracterization as pure anarchy. A more fragmented Internet and digital ecosystem could occur in the future if the vulnerabilities resulting from interdependence were no longer outweighed by benefits.

The discussion made clear the need for additional thought concerning how to measure the impact of different strategies – including deterrence, but also persistent engagement and efforts at norm establishment. How can we measure changes in the degree or character of adversary cyber aggression that might result from our own strategic choices? This has implications not only for measuring the success of deterrence, but also of strategies involving "persistent engagement" and "defending forward," and of norm development efforts. Such metrics are necessary in order to evaluate the success of current strategic shifts.

Discussion also indicated several areas where cyber diplomacy and multi-stakeholder engagement might be of continuing importance. This included need for greater understanding of adversary concepts, escalation ladders, and threat perceptions – both to reduce risk of misperception-fueled escalation and to prevent strategic surprise. In highlighting the importance of the technical and operational architecture of the Internet and other digital infrastructure in structuring the cyberspace environment in which competition occurs, the discussion also suggested the potential importance of ongoing dialogue with relevant stakeholders from the private sector and technical communities.

Overall, the discussion indicated that there is still significant lack of clarity or consensus on how best to approach cyber strategy in connection with increased great power competition. Any appropriate effort to address these shortcomings must account for the cyber domain's unique characteristics, including its often covert nature, its frequent exploitation during peacetime and grey zone conflict, its overlap both with technical systems across domains and with globally interdependent civilian infrastructure, and its potential impact on the economic, media, and political systems of liberal democracies. If a more mature cyber strategy aims for stability while denying strategic gains by competitors, and involves significant engagement in a space below the threshold of armed conflict, it may look very different from prior strategic models

developed for other domains. Concepts and comparisons must be carefully considered to avoid basing lessons on false analogies.

Panel 2: Cyber Competition and the Changing Strategic Environment

- How do Russia, China, North Korea, Iran and other key actors operate in cyberspace and conceptualize its role in broader forms of military, economic, and political competition?
- How do they conceive the different requirements of cyberspace operations in peacetime, crisis, and war?
- How has cyber competition affected the international security environment so far? How is this likely to develop in the future in the face of new and emerging digital technologies and the proliferation of cyber capabilities?

The second session examined the role of cyber competition in today's changing global strategic environment. Focusing on the evolving strategies of key current actors, participants considered how competitors' cyber strategies relate to their larger policy objectives and threat perceptions. The discussion addressed important differences in the conceptual lenses through which the United States' competitors view the cyber domain, often including greater emphasis on information control, economic gains, and supply chain vulnerabilities.

Examination of Chinese cyber strategy, for example, noted how the country views cyber as an effective tool for policy goals from controlling escalation to maintaining social stability. In terms of military applications, a greater integration of cyber capacity has been in part born out of the realization that China's nuclear No First Use posture did not serve as a credible deterrent for non-nuclear war. To that end, some recent Chinese military exercises have included the use of offensive cyber capabilities. Structural changes in China's force posture include the 2015 reorganization of both offensive and espionage cyber units into the Strategic Support Force of the People's Liberation Army. There has also been increased central oversight of cyber operations and a crackdown on government personnel hacking for personal profit.

China's main concerns in the cyber domain, it was suggested, are reliance on foreign ICT (particularly following the Snowden revelations), arms racing with the United States, and its own growing vulnerability to cyberattacks. As China's population comes to increasingly use and rely on the Internet and digital technologies, the Chinese government perceives a greater vulnerability to both destructive cyberattacks and broader societal upheaval. China has tighter control over domestic online discourse than most non-democracies, having built censorship into its Internet architecture from its early development; but this very architecture of control could also be proved vulnerable. China believes that the United States played a role in the 2011 Arab Spring and fears foreign interference over social media. In general, China has grown out of its previous self-perception of extreme vulnerability in cyberspace but does not yet see itself at parity with the United States.

Participants noted how Russia also views cyber as a component of a broader information control strategy, though with some differences in precise characteristics and relation to broader military strategy. In contrast to the United States' focus on technical cyber operations, Russia focuses on control and distribution of information through any means, including cyber. This draws on elements of earlier Russian and Soviet strategy such as "reflexive control," with an interest in psychological manipulation to affect decision making processes, but it also integrates the use of new digital information systems. Like China, Russian strategy has been affected by concern about domestic stability and a fear of Arab Spring type events such as the Color Revolutions that have occurred in neighboring countries. The approach is reflected in the writings of General Valery Gerasimov, focusing particularly on significant strategic gains that can be achieved through peacetime and grey zone activity. Russia sees cyber and cyber-enabled information operations as integral to this new kind of competition.

Russian use of cyber operations was also connected to the country's larger geopolitical objectives and threat perceptions. Russia was described by some as a highly revisionist power not satisfied with the status quo and seeking to undermine aspects of the rules-based international order through activities like fait accompli attacks, election meddling, and other forms of sub-threshold or covert operations meant to achieve aggregate gains of strategic significance. Participants also discussed a threat perception which held the Soviet collapse and later 2011-2012 domestic mass protest mobilization as possible results of adversarial information operations, NATO expansion as a form of neo-containment, the Russian people as historical saviors of Europe, and a generally zero-sum view of geopolitical competition. The country also has faced a renewed recent wave of domestic protests. It was suggested that the administration of President Vladimir Putin is concerned by potential political repercussions of worsening economic conditions and might engage in cyber operations to avert further unfavorable economic changes with negative impacts on domestic legitimacy. For the moment, Russia's recently-adopted "Internet sovereignty law" seeks to move Russian Internet control closer to that of China, permitting authorities to more tightly censor banned content and implement a "kill switch" to shutdown the Internet in moments of crisis.

Some participants suggested that the current lack of trust between governments such as the United States, Russia, and China makes fruitful negotiations on cyber norms challenging. The repercussions of failures to communicate or understand adversary strategic concepts and threat perceptions were also noted. Some suggested that the relative vulnerability of each state to cyberattacks might also be shifting, as they pursue greater networking and connectivity through the Internet of Things, compete in the development of Artificial Intelligence (AI) capabilities that could influence offense and defense capabilities in both cyber and information operations, and implement their various approaches to Internet content regulation.

Participants discussed the growing cyber capabilities and use of cyber and cyber-enabled information operations by countries in the Middle East. Understanding the role of the cyber domain in the Middle East depends on the lens through which the region is viewed. One lens discussed was that of great power competition, viewing the region as the site of influence campaigns by great powers, the source of threats such as terrorism and nuclear proliferation, a

source of strategic utility via geography or resources, and the site of ideological partnerships. Discussion also looked at the Middle East through the lens of regional states and their interests, revealing a different picture for the use of cyber operations. Middle Eastern states themselves are primarily concerned with domestic issues, particularly after the Arab Spring. While some states in the region continue to develop cyber military capabilities and have begun to use these capabilities to target the United States or its allies, preventing civil unrest and maintaining regime stability remain key interests. We also see cyber and information operations being increasingly used in intraregional competition.

Iran is often indicated as one of the leading adversarial cyber domain competitors behind Russia and China. From an Iranian perspective, it was suggested, cyber represents not a path to dominance but a response and deterrent to U.S. dominance. Stuxnet and the Snowden revelations led to a much greater Iranian focus on offensive cyber operations beyond domestic surveillance, with the recent Iranian intrusion into a U.S. dam as an example of this shift. Iran has also been trying its hand at information operations, both in its immediate region and in Europe and the United States.

New dynamics of cyber in the Middle East that were noted as bearing continued attention include the growing investment by Gulf Cooperation Council (GCC) states into AI and commercial dual-use cyber technology, and the potential for non-state actors to quickly mature in this environment. Furthermore, while the Arab Spring was aided by the Internet, the underlying social issues that prompted it (e.g. poverty, lack of access to education, authoritarianism) remain present and could surface again, in ways permutated by both citizens' and governments' greater adoption of technology.

Panel 3: Cyber's Place in Integrated Strategic Deterrence

- What role does the cyber domain play in integrated strategic deterrence, following the reassignment of the mission from STRATCOM to CYBERCOM? What role can and should it play?
- What are the respective roles of deterrence, persistent engagement, and norms-based strategies in the cyber domain at different levels of conflict? Where is there disagreement about the risks and merits of approaches?
- What more thinking about cyber strategy should be done? By whom?

This session addressed the place of cyber strategy in relation to overall defense posture and to competition within the cyber domain. Much of the discussion revolved around the alternative strategic concepts of deterrence, persistent engagement, and norms development that are currently being analyzed by the U.S. Cyber Solarium Commission. This commission was created by the 2019 National Defense Authorization Act, in keeping with the National Defense Strategy Commission's recommendation that "Congress appoint a high-level commission to review U.S. cyber policy." The NDSC noted the problem that efforts to defend the U.S. against and respond to frequent cyberattacks by adversaries are "hamstrung by debates over authorities and

jurisdictional boundaries." In addressing these issues, they suggested such a commission would "offer recommendations on how to streamline decision-making and bureaucratic processes, while protecting civil liberties and leading efforts to establish international cyber norms."[1]

Considering the role of the cyber domain in integrated strategic deterrence raised questions of how cyber operations might uniquely contribute to deterrence, and what types of actions such operations might deter. U.S. deterrence messaging is often threatening but vague, which allows latitude to use a variety of tools. Participants considered how cyber effects might be part of a broader package of nonlethal, lethal, or catastrophic means of response. While it might be most obvious to utilize cyber means in response to a cyberattack, other plausible uses might be in reaction to nonlethal uses of force in other domains—an option perhaps demonstrated by the recent cyber response to the Iranian shoot-down of a U.S. drone. Contemplating a potential firebreak between lethal and nonlethal war raises questions about how to effectively deter the threat of militarily consequential but nonlethal attacks that might devastate a country's ability to fight but leave no casualties. For example, some mix of cyber, electronic, information, and space-based warfare could render a country defenseless but remain well below the firebreak of lethal war.

Discussion also examined the possibility of deterring attacks within the cyber domain. Offensive cyber operations complicate traditional theories of deterrence, although what aspects can be carried over to the cyber domain and what strategies are implied by the complication remain subjects of heavy debate. Deterrence by punishment relies on the ability to set clear thresholds for provocation that will incur a response. However, the record of state cyber operations does not offer easy examples of which non-cyber provocations naturally invite a cyber response. The difficulty of establishing this linkage between provocation and response, and therefore defining a threshold, undermines a key basis for deterrence. Additionally, states' cyber capabilities are unclear if not exercised, so signals of capability will often lack credibility. Even when states exercise their capabilities, those capabilities are still uncertain to all besides the attacker and victim—and the victim may not be able to ascertain whether the attack worked as intended, if the attack was intentional at all, and what the attacker intended to signal with the attack. Too clear a signal about a cyber deterrent can lead to discovery, thereby eliminating the deterrent capability. Lastly, deterrence rests on the ability to continuously hold targets at risk, which is difficult given the fragility of access in cyberspace—everything from a scheduled patch to an unanticipated natural disaster can disrupt access and therefore deterrence.

Participants also discussed how deterrence by denial could function in cyber, with significantly divergent views on how denial relates to defensive signaling and whether it can play a significant role in the cyber domain. It was argued that the relatively high cost-effectiveness of offensive cyber operations along with the difficulty of ascertaining defensive capabilities undermine deterrence by denial in cyberspace. In other words, since attackers pay so little to conduct an attack and often cannot know the strength of defenses, there is little to dissuade

[1] National Defense Strategy Commission Report, November 2018. https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf

them from trying. However, some suggested this need not be a permanent feature of the domain, with AI and active defensive measures potentially shifting the offense-defense balance over time. Some even suggested that recent U.S. announcements of a strategic shift towards more forward defense could be seen as a form of deterrent signaling. Discussion also highlighted the value of increasing resilience and hardening defenses where possible: If cyberattacks cannot be entirely deterred or preempted, then surviving them with limited damage takes on more importance.

The benefits and some risks of the strategy of persistent engagement, as articulated in U.S. Cyber Command's 2018 Command Vision and other strategic documents, were a topic of significant interest. Advantages of adopting persistent engagement discussed included the constant signaling of capabilities and resolve, and the ability to achieve strategic effects without escalating into armed conflict. Participants also noted challenges to overcome in executing persistent engagement, including the risks of operator burnout due to increased operational tempo, and of expending capabilities faster than they can be developed.

While the new strategy has generally been associated with a rejection of deterrence, participants noted that current strategic thinking considers deterrence valid for the strategic space of armed conflict, emphasizing the pursuit of competition through persistent engagement below the threshold of armed conflict. There was some disagreement about the precise meaning and implications of this dual strategy, however. Some participants were concerned that the simultaneous pursuit of above-threshold deterrence and below-threshold persistent engagement might reduce signaling clarity, creating difficulty for victims of an intrusion to determine which space and strategy the intrusion was intended to serve. This confusion could be particularly destabilizing during a crisis or around systems that could plausibly be targeted for both below-threshold or above-threshold operations. Others held that above-threshold or below-threshold strategic intent would be obvious based on the systems targeted.

The discussion of competitive strategies in cyberspace raised the equally contentious issue of norms of state behavior, whether as a strategy in themselves or the products of applying other strategies. A central question was how norms are generated, and the relative explanatory power of public inter-state agreements versus repeated interactions generating publicly unacknowledged but mutually understood standards of behavior. Different answers to that question necessarily led to differing opinions on the approach states should take to develop norms favorable to their interests—whether states should engage in high-level diplomacy to enshrine formal norms, comport themselves according to the norms they want to generalize, or some mix of both. Participants eventually agreed that behavioral norms of some form result regardless of approach, though there is no guarantee they will be aligned with states' intentions or aspirations. Most agreed that, so far, states have shown little restraint in cyberspace short of armed conflict.

As this discussion made clear, the historical record of state behavior in cyberspace cannot be neatly separated between strategic approaches involving deterrence, persistent engagement,

and norms. Moreover, the relationships between these three approaches and their optimal combination in future strategy remain subjects of significant debate and will benefit from continued analysis.

Panel 4: Cyber's Place in Adversary Information Confrontation Strategies

- What are those strategies? How do their means and ends differ from Cold War propaganda strategies?
- Among the tools of information confrontation, what is the relative importance of cyber?
- What implications follow from the asymmetric vulnerabilities of democratic and non-democratic states to such strategies?

This discussion focused on contemporary adversary information confrontation strategies, comparisons to Cold-War-era analogues, the enabling roles of current information technologies, and the asymmetric interests and vulnerabilities of states of differing regime types. Participants explored tactics, capabilities, and implications, and discussed potential solutions to reduce the vulnerability of democratic societies.

Contemporary information confrontation tactics rely on many elements from the historical toolkit, including the dissemination of biased, false, or unfalsifiable information, often laundered through more reputable sources. These techniques can be combined with more overt forms of propaganda such as biased media outlets, or with other forms of covert operations. They are particularly valuable for influencing behavior and outcomes in peacetime and grey zone conflicts. As much as contemporary digital information operations can seem novel, participants reviewed the many similarities and high sophistication of earlier applications. Some suggested, for example, that current Russian information confrontation strategy is largely congruent to that of the Soviet Union, which sought to create discord and confusion around targeted issues and alter a rival's decision-making processes. Such operations, with roots in Soviet models of "reflexive control," utilized psychological vulnerabilities and biases to plant the seeds of uncertainty and tension around the choice itself. Russian actors are flexible and opportunistic, with their operations frequently uncovering new opportunities which can be seized and used for other activities, such as quickly pivoting from political espionage to hack-and-leak.

Despite the clear similarities, many agreed that today's digital ecosystem has changed the nature of what is possible. Online platforms and algorithms allow cheap, rapid, scalable execution of these tactics with targeted operations possible across larger portions of society. Participants discussed how the current moment of technological change has increased audience difficulties in distinguishing authoritative sources, helping enable a range of information confrontation strategies. The tools of today's disintermediated information ecosystem—from user data sharing, search engine optimization, and anonymous handles, to targeted advertising, user-centered search, and content recommendation engines—allow the easy dissemination and amplification of disinformation targeted at susceptible populations.

From polished but biased outlets such as RT (and its many YouTube stations) to fake activist group sites or extremist social media accounts, these techniques often seek to exacerbate existing divisions and polarization in society and rely on unknowing Internet users for their spread and credibility.

Part of the difficulty of dealing with these types of adversary strategies is conceptual. Operations like these that utilize networks and computer systems to spread information, or "soft" cyber, are often considered distinct from "hard" cyber operations interfering with the basic functions of computer systems. In spite of its own Cold War history dealing with adversarial psychological and information operations, the United States has been concerned mostly with "hard" cyber and the technical aspects of computer systems and networks in its cyber strategy. Cyberattacks have been understood to involve hacking, breaking things, and exploiting technical vulnerabilities. Similarly, cybersecurity has been viewed through the lens of the "CIA framework,"or maintaining the confidentiality, integrity, and accessibility of data.

However, some states have long conceptualized the cyber domain differently, viewing information content and digital technologies as part of a common domain. Russian operations, for example—like hacking an Iranian APT group for false-flag operations, disrupting critical election infrastructure to undermine trust in government, leaking confidential emails to influence media coverage, or spreading disinformation on social media with fake accounts and algorithmic targeting—clearly reflect an approach integrating both hard and soft cyber. This integration is seen in the broader stances of countries like Russia, China, and Iran on Internet governance. Perceiving the digital spread of certain types of information and organizing as severe threats to their own regime stability and national security, they promote "Internet sovereignty" as the extension of political control over online interactions and discourse. They similarly pursue political aims abroad through both hard and soft cyber. Other states like the GCC members are attempting to realize a similar approach, though their capabilities are more limited due to current technological disparities. Notably, many non-democratic regimes first test out these information confrontation techniques against their domestic opponents before employing them abroad. Governments learn from the demonstration of techniques by early adopters elsewhere, and some of the accompanying technical tools or services are available for purchase through global markets.

Despite significant national efforts at defending against hard cyber, the United States has been more vulnerable to soft cyber operations. The first wide-scale deployments of cyber-enabled information confrontation techniques came as a strategic surprise to a community focused more on defending against cyber-to-kinetic threats to critical infrastructure than against the hijacking of social media to influence public discourse. Many participants also agreed that democratic states are most vulnerable to these types of operations due to inherent differences in their governing structures, the value attached to freedom of expression, media, and association, and the independence of private sector companies such as social media platforms and search engines. More authoritarian governments often have a greater capability to control information flows, through a mixture of restrictive laws, censorship, Internet shutdowns,

pervasive surveillance, control over intermediary platforms, and manipulative content production.

It remains a topic of open debate whether the greatest burden of response to cyber-enabled information operations in democratic countries should fall on the military and national security communities (e.g. through deterrence, persistent engagement, and other outward-facing strategies), the private sector (e.g. algorithm adjustments, or changing terms of service), domestic government (e.g. regulation of social media platforms), or civil society and the education system (e.g. media literacy initiatives). Currently different alternatives are being explored by the United States and allied countries. With the ongoing development of sophisticated AI-based techniques like deepfakes, sentiment analysis, and micro-targeting, as well as the proliferating use of these techniques by a wider set of actors, few saw this challenge being fully resolved for the foreseeable future. On the other hand, some also expressed concerns about solutions worse than the disease, including worries about democratic states mirror-imaging non-democratic cyber domain concepts in ways at odds with their core values, or a growing encroachment on freedom of expression.

Panel 5: Managing the Risks of Cyber Competition

- What role, if any, can formal legal measures, negotiated among competitors, play in managing risks? What role can informal mechanisms play, including but not limited to norm creation?
- What impact are the law of war and the just war tradition likely to have in restraining cyber war and cyber competition? What about economic and social interdependencies?
- What unique risks and governance challenges are posed by conflict and competition in cyberspace? Are there relevant roles for non-state stakeholders, international institutions, or alternative governance models?

The fifth session examined what processes could allow states and other actors to manage risks inherent in cyber competition. Discussion included the current and potential future roles of formal legal measures like treaties and the law of armed conflict; informal processes such as norm development; and the impact of economic, social, and technical interdependencies. The roles of various non-state stakeholders in Internet and technical governance—and potential resulting influence on the cyber domain—were also considered.

Participants acknowledged the significant efforts that have been made by a variety of actors to clarify the role of international law in cyberspace and to influence the development of cyber norms. These include the development of the Tallinn Manuals, work of the Global Commission on the Stability of Cyberspace, multiple United Nations Group of Governmental Experts (GGE) processes, and the UN's Open-Ended Working Group (OEWG). Despite these efforts, many communities retain deep skepticism of their utility.

As understood in the study of international politics, norms are "expectations of proper behavior by actors with a given identity."[2] But alternate understandings in different communities within the cyber policy space have yielded not a little confusion. First, in keeping with the social science definition, norms do not need to be the product of official state negotiations but rather can come from repeated action or restraint. Second, norms are often informal and multi-actor. Finally, though many use the word only when discussing aspirational standards, norms in the social science understanding are value-neutral. Some forms of norms already exist in the cyber domain, emerging from prevalent behaviors. These can even result from design decisions embedded in technology, like technical standards or functionalities, and inherently constrain use options. The question is whether these existing norms are also the norms best suited to managing the risks of cyber competition, and, if not, how such risk-mitigating norms could be developed.

Here the discussion acknowledged the relationship between the two understandings of the term "norm:" some formal norms are not yet descriptive, since they do not reflect behavior, while some descriptive norms have never been formally enshrined. Any move from formal to descriptive norms is not preordained, but can be achieved through norm entrepreneurship. Whether through spearheading a formal agreement or mobilizing transnational activism and publicity campaigns around an issue, various actors can act as norm entrepreneurs, using incentives and interests as well as value beliefs to prompt buy-in.

Though the conversation about norms sometimes confounds the difference between the "logic of consequence" (one does not commit a crime because one will be punished), and the "logic of appropriateness" (one does not commit a crime because one considers it inherently wrong), both logics can play important roles in norm development. Actors often obey a norm first out of consequence, then out of appropriateness as the norms are entrenched and internalized. Again, such a progression is far from inevitable. The "cyber norms" discussion is usually focused on efforts to build new norms that restrain states from cyber operations of which they are capable and which are otherwise in their interests. The question is whether such aspirational norms are currently achievable – whether through formal agreements or otherwise. Some participants noted that in choosing aspirational norms, it is useful to set goals that are not so far from current behavior as to be unachievable. Setting the bar too high and failing could lead to broader cynicism around the entire process.

To a greater degree than in other domains, the private sector and other non-state stakeholders have actively sought to influence cyber norm development. Cyberspace – and thus the cyber domain – is heavily influenced and controlled by the private sector. In addition to activities involving purely government or military assets, adversaries often use vulnerabilities found in software code, false accounts on social media networks, or critical infrastructure owned and operated by private companies. Technical experts and civil society also play important roles through Internet governance institutions and technical standards selection. The private sector

[2] Finnemore & Hollis: https://www.iilj.org/wp-content/uploads/2017/01/Finnemore-Hollis-Constructing-Norms-for-Global-Cybersecurity.pdf

has spearheaded a number of norm-building efforts: for example, the Cybersecurity Tech Accord and Paris Call for Trust and Security in Cyberspace, both authored by Microsoft, and the Charter of Trust, authored by Siemens, seek to establish stabilizing norms in the private sector in order to promote similar norms throughout all sectors of the cyber domain. While some participants considered such initiatives helpful for limiting risk, others remained unconvinced that they meaningfully challenged the dominance of governments. Participants also pointed out that the relationship between the government and the private sector is radically different in the United States compared to that in competitors like China and Russia. Thus, the establishment of norms cannot hinge entirely on intra-private sector agreements.

The policy of persistent engagement also factored heavily in this discussion; particularly whether persistent engagement (or some form of below-threshold, unrestrained offensive behavior) is already an international norm today, how exactly it might be used to shape norms, and what norms would be likely to develop if the United States pursues a policy of persistent engagement. While some in the discussion expressed concerns that persistent engagement may further normalize the weaponization of cyberspace and encourage the proliferation of offensive cyber capabilities, others suggested that persistent engagement operations could be used as a method of constructing norms within a space of "agreed competition." This raised questions about the specific mechanisms by which these operations could influence norms, and the types of aspirational norms that persistent engagement should seek to foster.

A related concern regarded the impact of persistent engagement's more assertive approach to cyber competition on U.S. alliances. Citing the inability of some allies to develop offensive capabilities, uncertainty about U.S. offensive (as opposed to defensive) cyber cooperation, and uncertain U.S. tolerance of allies defending forward in U.S. networks, some suggested persistent engagement risks being perceived as a double standard.

Participants also expressed concern regarding the need for some forms of dialogue or effective signaling, questioning whether offensive and forward defense operations alone could effectively be used to reduce risk and establish desirable norms of behavior. They argued that signaling is vital to the development of stabilizing norms, and highlighted unfavorably the apparent unwillingness of states to establish redlines or constraints on their own actions in cyberspace. Some participants suggested that the diplomatic dialogue surrounding norms can force states to clarify redlines that would remain ambiguous otherwise, and therefore may be worth having even if it yields no appreciable change in behavior.

Panel 6: U.S. Allies as Co-Competitors

- What can allies contribute to cyber competition? How can they help to out-think and out-innovate cyber competitors?
- How has NATO approached the cyber challenge? How have allies and partners in Asia?
- What particular equities of theirs should the United States government understand?

This session discussed the current roles of U.S. alliances in cyber competition, the ways in which this collaboration could be strengthened, and the challenges it faces. There was general agreement that alliances are a key part of effective action in cyberspace and that the scope of operational, legal, and normative objectives being contemplated can only be achieved through cooperation. However, each country's differing priorities (e.g., security vs economic prosperity) and policies toward international norms, legal obligations, or the role of government complicate a fully unified approach to cyber activities. While the United States and its allies often agree on the nature of the threats and recognize the need for cooperation, participants also found that the cyber domain offers a unique set of challenges to inter-alliance dynamics, including economic interdependence, varying deterrence postures, and a lack of like-mindedness on cyber norms.

The discussion highlighted several important ways in which allies can contribute to cyber competition irrespective of cyber capabilities or resource level. Broad alliances like NATO allow for experimentation among allies on cyber strategies and doctrine, with mechanisms to allow the sharing of best practices. Allies can help share the costs of technology development for expensive initiatives like quantum computing. Japan's ability to build, service, and support technology infrastructure like 5G alternatives and secure data transmission cables as well as R&D on emerging technologies was noted as an example.

In confronting adversary behavior, presenting a unified front can also be beneficial provided the necessary coordination has been done. This helps undermine the narrative that the United States is orchestrating a plot to undermine the other country or actor and reinforces the sense of common cause among allies. The example was given of hard lines taken by Australia and other allies on the national security risks of Huawei products. But the varying economic and security equities of different allies has prevented full agreement on this issue.

Another valuable contribution is sharing expertise and best practices as a way of bolstering cyber resilience collectively as well as individually. As one participant noted, small cyber exercises can go a long way. Intelligence sharing can also be an important aspect of cooperation, though easier in some alliance relationships than others. It was explained that even the Five Eyes intelligence alliance between the U.S., Australia, Canada, New Zealand, and the United Kingdom, has shown signs of strain in adapting their operational and intelligence sharing heritage to the demands of cyberspace.

Extending cooperation down to the tactical level, especially in multilateral alliances like NATO, has the inherent limitation that the alliance is a reflection of states rather than a substitute for them. When it comes to collective action, NATO relies on constituent nations to provide "voluntary national effects" when relevant, and be their own first line of defense in identifying threats. If a threat is identified, that nation must bring the threat to the attention of the allies together and present a convincing case for why it is an alliance problem in need of action.

Cyber competition also presents certain limits to alliance cooperation. Participants questioned how extended deterrence could apply to the cyber domain if at all, and several noted that current worries in some allies about the U.S. commitment to extended nuclear deterrence are only magnified in the cyber domain, where commitment is even harder to signal. Some also worry that defensive provisions from high capability countries will disincentivize cyber development among allies who still need to build their own capabilities. A second order concern stemming from this was the effect of cyber assurance exacerbating the security dilemma with current or potential adversaries who may become motivated to escalate in order to address the forces of the nation extending the assurance. Thus, some workshop participants were of the view that alliance members should independently build a minimum degree of native resilience and defense capability as a precursor to allied cyber cooperation.

In addition to concerns about the effects of U.S. persistent engagement on alliances, which were echoed from previous panels, the discussion also revealed that some allies differ from the United States on the clarity of redlines for cyber deterrence. While the discussion suggested that current U.S. strategy involves reaching clear mutual understandings of thresholds, other allies are pursuing an approach of deliberate strategic ambiguity regarding redlines in order to minimize adversary activity. The difference between these stances may not be clear to adversaries.

Other current and future sources of tension in alliances include economic interdependence, domestic applications of cyber tools, and different preferences for response options like public attribution. On economic interdependence, the Huawei issue demonstrates that different allies have different levels of economic entanglement with competitors like Russia and China, and therefore prefer a different balance between security and economic gains when participating in a joint approach. Some held that Chinese overseas activity becomes even more concerning as cyberspace norms begin to solidify; Chinese investment and influence may be instrumental in swinging the opinions of countries who have not yet taken a position on what those norms should be. Participants also discussed how U.S. allies like Egypt and the GCC states align much more closely with China and Russia in their employment of cyber for domestic information control, and that this could be a source of tension in these alliances going forward. Lastly, some allies suffer disproportionately from participation in responses like joint public attribution.

Panel 7: The Promise and Limits of Public-Private Cyber Partnerships

- How is cyber competition for national security changing civilian cyberspace and technology sector development?
- What can the private sector do to help out-think and out-innovate cyber competitors?
- What additional equities constrain and/or compel improved public-private partnership?
- How do relations between government and the private sector in potential adversary countries differ from those in the United States and its allies? What are the implications for cyber domain competition?

The seventh panel examined the role of public-private partnerships (PPPs) in enhancing national security in cyberspace from the perspective of the U.S. and allies. It looked at both the form of past and present partnerships between governments and the private sector and their purpose for maximizing security and realizing national strategic goals. This was compared with government-private sector relations in competitor countries.

Over the past decade, the number and complexity of public-private partnerships (PPPs) has grown to tackle problems of resources, manpower, and capability no side could overcome on their own in cyberspace. While participants remarked that this is not a new development, attempts at analyzing PPPs have largely focused on their form, (i.e. which actors are involved and how they relate to one another) and less on their function or purpose. Such a functionalist perspective reveals that actors generally enter PPPs for three reasons: (1) to achieve outcomes they cannot attain alone, (2) to tackle computational problems that are too complex to overcome independently, and (3) out of mutual and self-interest. Thus, entering into formal or informal partnerships with the private sector allows governments to achieve defense in depth, to operate globally and at scale, and extends their ability to exert sovereignty and project power. PPPs provide states with freedom of maneuver in cyberspace, situational awareness, and innovation to stay ahead of competitors. These benefits of PPPs are critical to realize persistent engagement and the defend forward posture outlined in recent cyber strategy documents—mass and scale enable persistent engagement, and knowledge and maneuverability enable a forward-leaning posture.

While some discussion of public-private partnerships focused on the benefits that working with the private sector can provide government, private sector actors also benefit from working with government. In some cases this has to do with financial benefits, but in others it concerns the defense of private sector networks and assets. PPP solutions are particularly attractive to small and medium-sized companies because of their relative inability to combat cyber threats compared to large, multinational companies.

PPPs can bring mutual benefits, but also come with risks and challenges. One perennial problem is the issue of trust between two actors who face fundamentally different incentive structures. Additionally, the legal policy frameworks regulating PPPs can stifle innovation and effectiveness when too rigid, or create divergence when partnerships are solely voluntary. Moreover, the question arises of who is ultimately in control of PPPs—while states tend to consider themselves in charge, they often depend on the infrastructure and sometimes on advanced capabilities that private sector actors bring to the partnership. Cultural tensions are at times significant. While the talent pool for government employment is national, the talent pools for the private sector and the elite universities that feed it are global. Universities and private companies increasingly face pressures to consider the risks of admitting or hiring citizens of competitor countries, but immigrants are often a significant demographic in the technology private sector.

Beyond the evolution of PPPs in cyberspace, this session also explored how the roles of private cybersecurity actors have shifted in recent years, both at the workforce and market levels. At a

market level, the development of greater capabilities in the private sector has occurred in part because private sector networks have largely had to provide for their own security as governments prioritized the defense of critical assets. Private cybersecurity firms market products and services to both companies and the government. In terms of workforce, private cybersecurity firms have successfully attracted former military and intelligence personnel through better paychecks and lifestyle differences. One perennial complaint from private companies is the illegality of certain forms of active defense measures that would allow them to better protect their assets by following or responding to aggressors outside their networks. The Active Cyber Defense Certainty Act currently under consideration in the U.S. Congress would regulate when private sector victims of hacking can self-defend outside of their own networks, permitting some of these measures. Legalizing "hack-back" raises further questions about the talent pipeline: If government employment loses its (current) unique appeal of being the only place where operators can legally learn and apply offensive skills, it threatens to increase difficulties in public sector talent acquisition.

How private cybersecurity actors use deception to counter attackers has also changed recently. Whereas earlier deception techniques were used to detect intruders, there is a growing market of companies leveraging deception to lure attackers into networks and gather intelligence about their routines and capabilities. Similarly, private-sector actors increasingly offer exploitation and espionage services beyond traditional corporate espionage. Former military and intelligence community employees with expertise in offensive and defense cyber operations and their employers increasingly capitalize on previous government affiliations to benefit from contracts with clients in the public and private sectors, within the United States and abroad—sometimes with considerable political and security implications. GCC states seem to be particularly eager for such services to amplify their ability to exercise power abroad and consolidate authoritarian rule at home. The question arises whether the increasing prevalence of highly experienced cybersecurity firms around the world distributes "cyber power" more equally among states, and whether this increases or decreases stability in cyberspace. Furthermore, the question was raised whether we will eventually see cyber mercenary-on-mercenary activities or cybersecurity firms contracting with both sides of an international conflict.

Private sector cooperation is also playing a significant role in national strategies for defending against and countering cyber-enabled information operations. Beginning in 2018, for example, the European Commission funded an independent network of fact-checkers and spearheaded an EU-wide agreed-upon framework of self-regulation for Internet companies, the Code of Practice on Disinformation, signed by many important online platforms and advertisers. In the United States, the State Department's Global Engagement Center (GEC) leads U.S. government efforts to counter propaganda and disinformation both from international terrorist organizations and foreign countries. Its Technical Engagement Team (TET) works with industry, academia, and foreign partners to identify and implement technologies to assist in this effort.

Similar to the private sector, participants noted, U.S. state governments and civil society have also assumed a greater role in cybersecurity. Several states, for example, have created or are in

the process of creating National Guard units with cyber capabilities, with Michigan and Washington being highlighted as particularly innovative. Cybersecurity has gained renewed urgency among state governments with growing concerns over the vulnerability of election systems, for which state-level agencies and regulations are responsible. One workshop participant suggested that state governments might look at non-monetary incentives to compensate cyber defenders for their voluntary or part-time services. Cybersecurity initiatives based out of academic and not-for-profit institutions also promote innovative solutions to improve cybersecurity domestically and in cooperation with foreign government and private-sector actors. Their efforts to improve passive cyber defense through educating stakeholders and the broader public, moreover, could enhance deterrence by denial. On the flipside, the increasing pervasiveness of cyber, e.g., Internet of Things (IOT), may also contribute to a growing militarization and securitization of civil society in this regard.

Panel 8: Back to the Key Questions—a Roundtable Discussion

- How should we answer the key framing questions?
- What other new insights stand out?
- How can we best carry forward this effort?

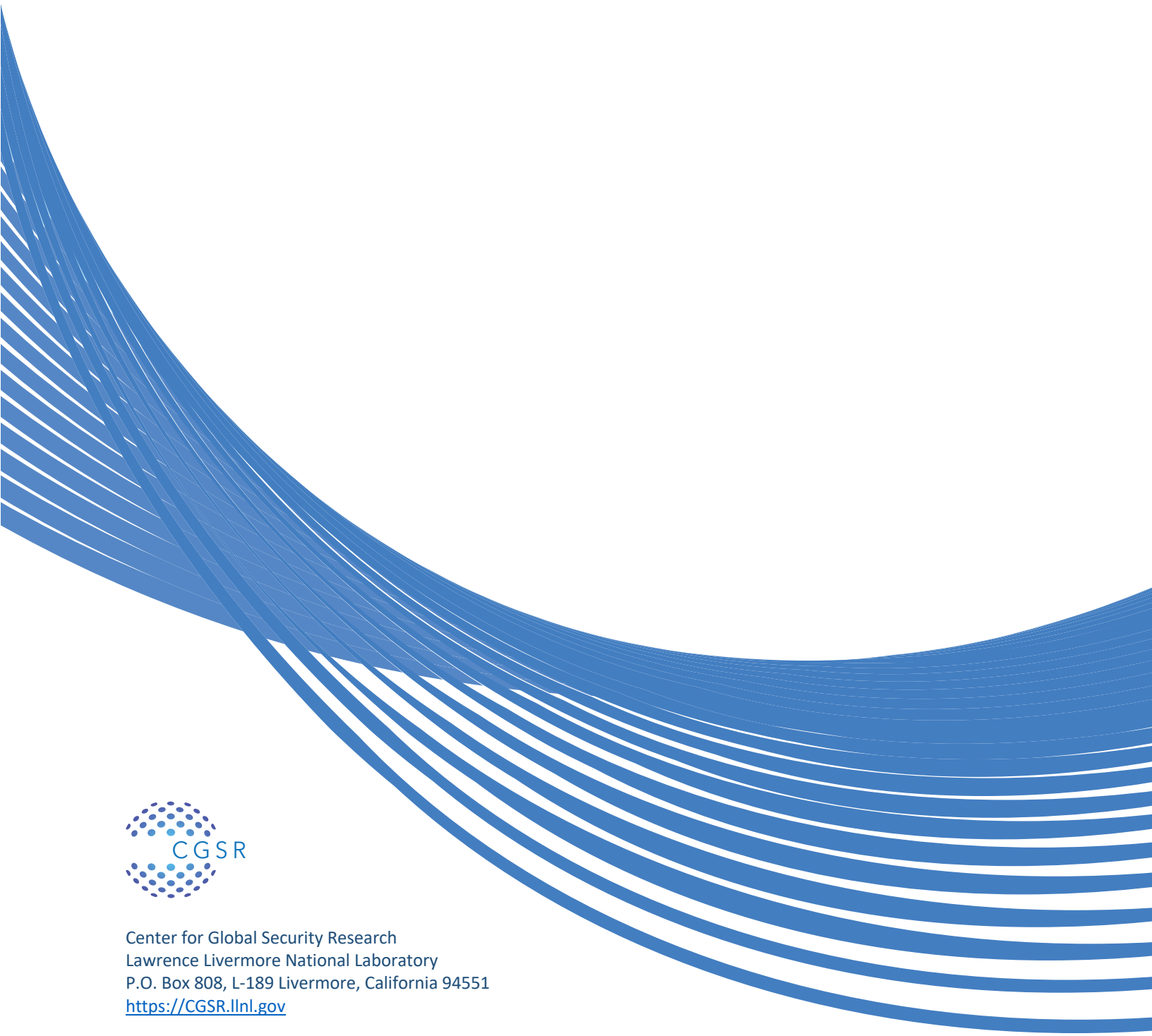
The conference concluded with a session that reviewed the workshop's findings and highlighted topics for further consideration. In revisiting the workshop's core questions, this conversation reviewed the themes of out-innovating, out-thinking, out-partnering, and out-maneuvering in the cyber domain as discussed by previous panels. Participants discussed key insights and areas in which additional work is needed in order to work towards these objectives and address the concerns of the National Defense Strategy Commission. Discussion examined the nature and implications of "over-match" and "strategic dominance," the degree to which sufficient operational concepts exist linking strategy with capabilities, and potential forms of risk that have so far been inadequately addressed.

One focus of discussion was on the conceptual lenses used by the United States and its competitors, and how these framings affect strategic thought often without our knowledge. For example, we tend to focus on the technical dimension over the strategic, and the technical over the psychological (in part because pure technology is easier to discuss). The three approaches of norms, persistent engagement, and deterrence have been considered as distinct and coequal conceptual alternatives, yet the boundaries between them are largely artificial. And at the widest lens possible, even the framing of the workshop was shown to reflect the U.S. focus on cyber *as a domain* rather than an approach integrating strategies across domains. Considering this, some noted the lack of focus on how cyber capabilities would be brought to bear in wartime situations, with much of the conversation having revolved around grey zone conflict.

Many participants also expressed the view that the meaning of competition, let alone its feasibility, was uncertain. It is unclear what the United States is competing for, especially because its potential competitors often see the domain through a completely different framework. Is competition for strategic dominance more desirable than establishing a balance

of power? A comparison was made to the nuclear domain in which the three main nuclear powers have largely abandoned the idea of seeking strategic advantage due to a shared recognition of its futility and possible danger. Not only does such mutual self-restraint seem for the moment unattainable in cyberspace, but the main players do not even agree on terminology and the "rules of the road." The question was raised what cooperative threat reduction would look like in the 21st century and in relation to cyber conflict, and whether some form of diplomatic or track 1.5 engagements could increase military cyber stability and decrease the risk of inadvertent escalation. More thinking, some argued, needs to be done on what distinct features of the United States constitute strategic advantages versus disadvantages. The recent faith in free flow of information only hurting authoritarian regimes bears remembering here. Lastly, there also remains a noticeable lack of operational concepts tying tactical actions to strategic goals.

Participants raised a diverse set of paths for future work. How should hypotheses be tested in the cyber domain, as the historical record of state actions lengthens and offers opportunities for study? How do high classification levels affect the possibility for successful research of this sort? If the threshold to entry is so low and strategic advantage can be gained, why do so many states seemingly choose *not* to compete in the cyber domain—why do we not see a record of cyber operations from the Cubas and Venezuelas of the world? Mirror-imaging, including studying how adversaries project their own self-perceptions onto the United States, is still understudied. Similarly, the roles of culture, private-public relationships, private sector innovations, economic interdependence, and how they differ between the United States and its adversaries all bear significantly on the cyber domain but are too often excluded. Participants agreed on the need to broaden the market for strategic thought, and widen the table at which it occurs: experts from economics, engineering, and social science disciplines all need inclusion to drive new strategic thinking in the cyber domain.



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-790304