Cyberspace, Information Strategy and International Security

Workshop Summary

April 2018

CGSR

Center for Global Security Research

LAWRENCE LIVERMORE NATIONAL LABORATORY

Workshop Summary

Cyberspace, Information Strategy and International Security

Center for Global Security Research, Lawrence Livermore National Laboratory
February 27-28, 2018

Prepared by Jaclyn Kerr, Rafael Loss, and Ryan Genzoli

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. How might increasingly competitive information strategies and military uses of cyberspace affect the security of the United States and its allies?
2. Who are the stakeholders in cyberspace security and what interests will shape their future choices?
3. What can be done to mitigate risks?

Context:

In recent years, the Center for Global Security Research has hosted a number of events to inform strategic thought on key areas of concern to national security and laboratory planning. This was the first dedicated workshop that CGSR has hosted seeking to convene a community of experts around issues of cybersecurity and Internet governance as they pertain to national security. The goal of this work was to bridge policy, academic, military, technical and other expert communities that often have limited contact with each other's concerns and specialized knowledge. This workshop brought together over 80 experts from government, military, national labs, academic institutions, think tanks, the private sector, and civil society and hailing from 10 countries.

While focusing on the national security challenges and military strategy emerging in and through cyberspace, the workshop aimed to address the cross-cutting interests and concerns of different stakeholders in the development and future governance of cyberspace, including those of the private sector, and civilian publics. To this end, the first day of the workshop focused particularly on issues directly relevant to military strategy in the cyber domain, while the second day addressed questions bridging national security and military concerns and their connections to the domestic and international politics of Internet governance.

Topics discussed included the evolving cyber strategies of the U.S., U.S. allies and potential adversaries, as well as the complex characteristics of the cyber domain, the potential for deterrence in or through cyberspace, the domain's escalation risks, and the ways in which the "dual use" nature of much of the underlying technology of cyberspace connects actions in the domain with broader questions of global Internet governance. Issues of online disinformation and information warfare and the unique conceptual tensions and governance challenges posed by these forms of conflict were addressed. The workshop also examined the roles and interests of different

stakeholders in addressing cybersecurity challenges, as well as the possibility of norms, international law, and other potential mechanisms of constraint.

Panel 1: Cyberspace and Security: Complexities of the Cyber Domain

- How has the cybersecurity problem evolved in U.S. defense strategy over the last two decades?
- How might it yet evolve? What are the main challenges ahead?
- How is military competition in this area affected by the unique characteristics of the cyber domain (i.e. dual use technologies, attribution challenges, multiplicity of actors)? How can we understand the relationship between the cyber domain and civilian cyberspace?

Even though cyberspace was viewed as a broad and somewhat disaggregated field, the utilization of cyber operations to support U.S. foreign policy objectives was recognized by many as essential. While noting the benefits of cyber weapons as generally safe and effective, usually low cost, and, as of today, non-lethal, participants also observed that the use of such weapons does carry a unique set of risks. Attacks in cyberspace have potential to create unintended consequences and be difficult to attribute to a specific actor, for example, increasing the potential for miscalculations. There is still significant confusion about thresholds, terminology, and the applicability of old concepts, with limited consensus as to what constitutes an "armed attack," "act of war," and the nature of proportional responses to cyber-attacks. The Internet's globally interconnected infrastructure and the complex relationship between the cyber domain and civilian cyberspace, furthermore, necessitate ongoing consideration of tradeoffs between interests in the overall Internet governance ecosystem. Despite such risks, it is clear that cyber operations will play an increasing role in future conflicts and global competition.

According to some workshop participants, U.S. strategy in cyberspace has been slow to evolve and frustration among the cyber and national security communities is growing. The Obama administration's strategy focused on three core areas: the digital economy, Internet governance, and Internet freedom. It also included three overarching objectives: 1) strengthening and defending U.S. Department of Defense (DoD) networks, 2) defending the U.S. homeland against cyber-attacks of serious consequence, and 3) providing cyber support to military operational and contingency plans. This strategy led to significant institutional growth, but was viewed by many participants as risk averse and primarily defensive in nature.[1] The strategy stated that the U.S. would "respond proportionally" to any attacks made in cyberspace, but mentioned little about offensive cyber operations. Participants pointed out that even overt actions in cyberspace against the U.S. during the Obama administration were barely punished, with some arguing this could lead to an increase in cyber-attacks, given the growing perception among adversaries that such operations are relatively "low risk." Russian interference during the 2016 U.S. presidential election - and the subsequent lack of a strong U.S. response - was cited as an example of such an overt operation against the United States that was minimally punished.

[1] Many cited a lack of focus on offensive operations as evidence to support their "risk averse" perception of the Obama administration's strategy. There was some disagreement among participants as to whether covert offensive operations during this period would qualify as "risk averse."

The arrival of the Trump administration left many in the defense community feeling confident that big changes in U.S. cyber strategy were ahead – and more specifically that emphasis would be placed on offensive cyber operations, along with stronger penalties levied against those responsible for attacking the U.S. According to participants, however, at the time of the workshop such changes had not yet materialized. Despite continued institution-building efforts and expanded authorities, including the elevation of Cyber Command to a full unified combatant command, at the moment of the workshop, many felt that doctrinal adaptations were still needed.[2]

The discussion highlighted several questions that should be explored during future strategic discussions. Some of these questions included:

- What organizations and institutions are best equipped to handle cyber issues?
- What is the role of the U.S. government and DoD in protecting critical infrastructure?
- What is the U.S. willing to risk during offensive cyber operations?
- What role will cyber play in how militaries fight future campaigns?

Participants also examined problems emerging from institutional legacies and stove-piping in the U.S., discussing possible paths to avoid post-crisis reactions. While institutional politics and inertia at times limit the ability to undertake sweeping change, efforts to innovate and think through solutions prior to crises can lay important groundwork to avoid less advantageous reactions when change is possible. In developing appropriate responses to threats in cyberspace, it was also recommended that more effort should be put into developing institutions that have the flexibility to adapt to conflicts as they develop.

Panel 2: Cyberspace in the Strategies of Potential Adversaries

- How do Russia and China think about and operate in cyberspace to contest U.S. power and interests? Do they make distinctions for different types of conflicts?
- How effective are these strategies and how might they develop further?
- What other actors pose the most serious threats in cyberspace now and in the future?

Both China and Russia have identified cyberspace as a strategic domain. As both continue to face challenges in leveraging the benefits of cyberspace while concurrently maintaining sustainable authoritarian regimes, they have embraced concepts of the new domain which include both cybersecurity and informational content. Both states continue to learn and adapt in efforts to manage forces within their societies and view potential threats to domestic political stability as among the most significant risks arising from cyberspace.

[2] US Cyber Command's March 23rd release of its new "Command Vision," three weeks after the workshop, arguably takes steps towards filling this gap. The new document, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," lays out a shift in strategic vision, embracing more offensive operations and ongoing contact within the cyber domain. It argues for "maneuvering seamlessly between defense and offense across the interconnected battlespace, " emphasizing "persistent action and competing more effectively below the level of armed conflict. "
https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf

Russia

Russian strategists conceptualize the cyber domain broadly, including computer network operations, electronic warfare, psychological operations, and information operations. Russia leverages cyber capabilities to influence domestic and international politics, and as mechanisms to support a broader strategy of information dominance. Russia uses many of these tools both during peacetime and conflict, both domestically and in the regional and international theaters. During peacetime operations, Russian cyber operatives utilize capabilities to influence political decision processes, alter public opinion, exploit social divisions, and undermine the credibility of political opponents. During armed conflict, Russia leverages the cyber domain for "grey zone" activities and covert operations in support of ground objectives. Operations often fluidly combine attacks on networks and data with cyber-enabled information campaigns.

The discussion highlighted salient examples of these various types of Russian operations, demonstrating how a mix of similar tools and tactics have been used in different contexts and theaters. During the Crimea annexation and Russia-Ukraine conflict, for example, Russian cyber operations were carried out to support a "grey zone" strategy and included information campaigns, attacks on critical infrastructure, and targeted surveillance operations – all enabled by and conducted through cyberspace. These operations exploited early attribution uncertainty, exacerbated unrest in the region, and sowed confusion at critical moments. Domestically, Russia sees "information security" as critical to regime stability. It leverages cyberspace to discredit political opponents, undermine protest mobilization efforts, and manage public discourse. Internationally, Russia exploits cyberspace to influence elections, undermine support for political parties and candidates, support extremism and polarization, and undermine the legitimacy of institutions not aligned with Russian foreign policy. Participants noted how Russia often leverages "hacktivists" and criminal networks as state proxies to conduct cyber operations, making it difficult to directly link attacks to the Russian government.

China

China aspires to become the most powerful nation in cyberspace and is currently working to improve its position and capabilities in the domain. The Peoples Republic of China (PRC) uses cyber operations as one tool among many to achieve information dominance, support state security, and to asymmetrically counter U.S. conventional military superiority. One participant noted that China is focused on ensuring that cyber technologies remain controlled by the government and places emphasis on regime stability in many of its activities. In addition to the significant control exercised over domestic Internet content, it was noted that many Chinese information operations conducted through cyberspace outside the country have primarily targeted Chinese ethnic communities abroad. From a military perspective, the People's Liberation Army (PLA) approach to cyberspace falls under the theory of "active defense," whereby offensive operations are conducted at the tactical level to support defensive postures at the strategic level. Additionally, as one participant stated, the PLA seeks to leverage civilian forces to conduct a "people's warfare in cyber space" in support of broader regional military objectives.

Cyber capabilities play a role in China's strategic deterrence strategies, and debates are currently underway to determine how effective cyber deterrence may be in the future. As one participant highlighted, the Chinese are exploring whether or not "firing a cyber shot across the bow" could deter adversaries from pursuing broader military action. In 2015, China established the Strategic

Support Force (SSF), bringing together its cyber, space, and electromagnetic capabilities under one roof. The SSF has two main combat forces; one for space operations and the other for cyber operations – the latter also includes both technical reconnaissance and electronic countermeasure brigades. As one participant noted, there is a big push in China to build future talent for cyberspace and the PRC is leveraging the commercial sector to support this effort.

Panel 3: Cyberspace in the Strategies of the United States and its Allies

- In U.S. military strategy, how are cyber capabilities expected to contribute to the achievement of U.S. objectives in peacetime, crisis, and war?
- How has this evolved over the last two decades and what challenges lie ahead?
- How have NATO and U.S. allies in the Asia-Pacific region approached security challenges in cyberspace?

The opening panel did much to lay the groundwork on discussion of U.S. cyber strategy and objectives. Participants acknowledged the significant work done during the Obama administration to clarify primary U.S. objectives and the roles of different government bodies in cyberspace, and to begin building institutions and strategy to meet these ends. But the discussion also pointed out ongoing shortcomings and challenges, as the boundaries between roles, limits on authorities, and emphasis on defense over offense left many concerned that segmentation, stove-piping, and risk-aversion had left the U.S. unprepared to effectively respond to and deter some forms of cyber-aggression. At the same time, conceptual vagueness and the potential for unintended consequences in the cyber domain cause ongoing concerns over misperception and escalation risks. The earlier discussion had introduced the connections between global Internet governance and cybersecurity policy. Recollecting the optimism about the global role of Internet freedom and the digital economy in the early 2010s, it emphasized the ongoing importance of these priorities and the need for norms and collaboration to protect the core global infrastructure that is the basis of civilian cyberspace. The third panel took off from these bases, focusing particularly on the developing institutions and strategies of U.S. allies and efforts at collaboration.

At the NATO Warsaw summit in 2016, the Alliance pledged "to ensure the Alliance keeps pace with the fast-evolving cyber threat landscape and that our nations will be capable of defending themselves in cyberspace as in the air, on land and at sea." The Allies committed to strengthen the defenses of Alliance and national infrastructures and networks as well as cyber defense capabilities and to enhance coordination, education and training, and information sharing. This pledge received senior-level attention within the Alliance. Cyberspace was recognized as a genuine domain in which NATO should be active and that cyber-defense is not merely a technical issue, but one of strategic and political importance. Ahead of the July 2018 NATO summit in Brussels, a review is underway to assess Allies' progress on the issue and NATO's role when malicious cyber activities so far have fallen below the Article IV and V thresholds, as was the case with Estonia in 2007.

Participants discussed challenges concerning the division of labor between NATO, the various European Union institutions, and national governments of member states. It was noted, for example, that the promotion of norms and governance structures for cyberspace is not within the NATO mandate and that individual member states are reluctant to reveal national-security relevant

cyber capabilities. Full transparency is probably neither a feasible nor desirable goal for NATO. Nevertheless, NATO has recognized that, to fulfill its purpose under the Washington treaty in the contemporary strategic environment, it has a role to play in the cyber domain as a signaling and capacity-building institution. It continues to provide a critical forum for member states to defuse disputes through regular exchanges at all levels and to engage with non-member states on issues of mutual concern.

U.S. allies in the Indo-Pacific are not inactive in cyberspace either. In 2017, Australia established an Information Warfare Division as part of its Joint Capabilities Group in an effort to integrate existing operations from across the Australian Defence Force to protect and support ADF personnel and systems. It has made an effort to provide more transparency regarding its approach to cyber operations, for instance, as it relates to organized cybercriminals. Australia sees its role as part of a coalition of the willing to promote norms for cyberspace and to overcome the collective (in)action problem plaguing the discourse on cybersecurity in the region. It also hopes to improve information sharing about malicious cyber activities in the region to prevent the Indo-Pacific becoming a testing group for cyber warfare. Though participants suggested that Chinese information warfare thus far has been limited to within China and ethnic-Chinese communities abroad, there also was concern that Russian-style election meddling might eventually be emulated in Asia.

Because of the self-defense clause in its constitution, Japan is more constrained in developing offensive cyber capabilities and doctrines. But the Japanese government does aim to create a cyber governance framework and capacity-building support program, providing an alternative for the countries of the Indo-Pacific to the model and capabilities promoted by China. Currently, several countries provide grants for cyber capacity-building, but this approach has so far been rather uncoordinated and eclectic. Efforts could be made to scale up these initiatives through multilateral cooperation.

Panel 4: Cybersecurity, Deterrence, and Strategic Stability

- Is deterrence in cyberspace possible? When? When not? Why?
- How might competition in cyberspace affect strategic stability with potential adversaries? How serious is the risk of unwanted escalation and how might it be reduced?
- Are there other risks that derive from the dual use nature of cyberspace and the global criticality of transnationally interconnected information and communications technology infrastructures?

There is currently significant contention over the best approaches to defending and maintaining the stability of cyberspace as well as concerning the role of the cyber domain in the deterrence or escalation of conflict. Debate over the possibility of deterrence in or through cyberspace highlights several areas of conceptual confusion and disagreement. "Cyber-deterrence" has been used to describe both the deterring of malicious cyber activity, as well as the achievement of broader deterrence goals through cyber means. It likewise has described both deterrence as strategy and deterrence as outcome and been discussed in relation to cyber-operations during times of warfare and those below the level of armed conflict outside the context of war. Workshop participants

discussed the need for greater clarity concerning the behavior to be deterred and the potential means for deterrence. While some research on cyber deterrence focuses on deterrence of malicious cyber activities by within-domain punishment, other work addresses a broader panoply of tools for de-incentivizing behaviors, including denial of effect, the development of norms, and mutual interdependence or "entanglement."

Workshop participants varied in their views on some of these conceptual distinctions and on the applicability of deterrence to cyber conflict, but there was a fair degree of agreement about the concerns to be addressed. Some argued that cyberspace, in its nature, is a domain of persistent action and ongoing contact between adversaries – characteristics precluding deterrence as an appropriate strategy for activities at least below a certain threshold of conflict. At the very least, it was suggested, deterrence through cyber means is unlikely to produce deterrent outcomes in isolation.

Traditionally, strategic effects, that impact a nation's resources to generate power, were accomplished through the violation of enemy territory. Through cumulative action, cyber operations now provide an alternative means to affect another nation's power resources. Accordingly, activities in cyberspace can undermine strategic stability. Cyber means are often employed below the threshold of all-out war. In the aggregate, it was argued, such sub-threshold actions can still have strategic effects, however. They also can potentially lead to inadvertent escalation, especially when cyber-attacks accidentally spread into other domains. Participants discussed how U.S. strategy should adjust to this persistent sub-threshold level of cyber contestation.

Given the nature of persistent and ongoing action in the cyber domain and doubts about the relevance of deterrence, workshop participants addressed alternative approaches to prevent inadvertent escalation and improve strategic stability. Active cyber defense was discussed as a possible means to deter malicious cyber activities against specific networks. The Active Cyber Defense Certainty Act (ACDC), recently introduced in the U.S. House of Representatives, would allow the use of limited, and potentially automatized, defensive measures that exceed the boundaries of one's network to monitor, identify and stop attackers. It remains open as to whether active and automated cyber defenses might relinquish some control over escalation, or in what ways it would be likely to impact intent signaling options.

Workshop participants addressed the cyber domain's serious escalatory risks, discussing the roles of perception and restraint and the likelihood of undesirable within-domain or cross-domain escalation. There is an inherent risk of misperception between actors in cyberspace, with intelligence gathering operations, signaling, and preparation for attack sometimes indistinguishable, and few clear rules of the road. Especially during crises, intentions might be easily misinterpreted. Some more hopeful research was presented suggesting that the cyber domain might not be quite as prone to inadvertent escalation as has been feared. Experiment test subjects have been reluctant to respond to cyber-attacks in other domains, potentially because of concern over loss of escalation control or the establishment of a detrimental precedent. Such behaviors and their causes in real scenarios are, of course, difficult to predict, and likely will differ across subject groups and over time. With mutual misperception still a serious risk in the new

domain, more research is needed to better understand the existing escalation risks and the cyber domain's broader potential impact on strategic stability.

As the role of the cyber domain in strategic competition between states grows, some have questioned the long term impact on the global Internet and civilian cyberspace. The discussion highlighted how issues of stability in cyberspace relate to global Internet governance and the interests of different stakeholders, examining a possible path forward for balancing the interests of different actors. The idea of a "Cyber Helsinki," considers cyberspace as a "regime complex" of multiple interrelated regimes, each with its own norms, principles, and procedures and occupied by a multitude of actors from the technical community, governments, the private sector, and civil society. To strike a balance between the interests of actors and legitimacy of norms, the proposal would mirror the multi-basket approach of the Helsinki process to promote norms concerning cybersecurity, digital economy, human rights, and technology, and to enhance communication and coordination around these issues. While challenges arise due to tensions between the core interests of different stakeholders and the complex relationships between issues, such a process, it was suggested, can be stabilizing even though no participant is likely to be fully satisfied.

Panel 5: Information Warfare Present and Future

- How should we think about strategic uses of information through cyberspace beyond the traditional understanding of cyber operations? How might this evolve in the future?
- How do cyberspace- and information-related security concerns and vulnerabilities of democratic and authoritarian states differ and how has this impacted their approaches to cyberspace?
- What approaches are currently being taken or should be taken by the U.S. and its allies to safeguard against or deter information and influence campaigns? What are the risks of addressing such problems as military concerns in democracies?

The current and emerging threats in the information environment go beyond the scope of traditional Western understandings of "cybersecurity." While recent events including the Russian meddling in the 2016 U.S. election and the extremist violence in Charlottesville, Virginia have drawn attention to the roles of Internet and social media content as potentially weaponizable or threatening to the foundations of democracy, there is a tremendous absence of conceptual clarity in the public discussion of these issues. A clear understanding of the problem and of how it relates to and differs from more traditional notions of cybersecurity and cyber warfare is critical to being able to address it and find effective solutions. Official U.S. Government definitions of cybersecurity have usually been framed in terms of the protection of computers and digital networks from attacks, and ensuring the availability, integrity, and confidentiality of data. While this conceptual framework is appropriate for discussing events such as the Russian hacking of emails and probing of election infrastructure, it falls short for describing other more overt activities which actually leverage the intended uses of information technologies and target human minds and social processes rather than computers, exploiting cognitive biases, social cleavages, and other flaws in society to achieve pernicious objectives.

Discussing the types of informational threats being seen today, the session explored alternative conceptual frameworks for understanding these strategic uses of information through cyberspace

that are poorly captured by the narrow "cybersecurity" conceptualization. A great deal of attention has rightly focused on the threat of foreign information and influence operations by adversary states such as Russia's use of trolls, disinformation, doxing, and targeted advertising in apparent efforts to influence public opinion, amplify polarization, and affect electoral outcomes in the U.S. and elsewhere. But the discussion also highlighted the significance of other threats including the use of "computational propaganda" and "information operations" by other actors for the promotion of extremist ideologies, terrorist recruitment, and for purposes of intimidation, bullying, and hate speech. Some mix of these tools are being used by many different actors, both state and non-state, domestically and internationally. They give rise to conspiracy theories, galvanize in-group/out-group sentiments, reinforce echo-chambers, exacerbate societal divisions, and fuel corrosive distrust in public institutions and political processes.

While there was debate among workshop participants as to whether these current problems should be regarded as fundamentally new, the discussion highlighted a number of mechanisms whereby the new digital information ecosystem enables qualitatively different behavior patterns than earlier eras of information operations or media disintermediation. Today's information campaigns benefit from the high connectivity, low latency environment that facilitates rapid, cheap, often-anonymous flows of information and communications. As opposed to many 20th century propaganda campaigns involving the top-down centralized dissemination of uniform content, the current forms of "participatory propaganda," often involve engaging audiences through deliberate precise targeting with tailored content that will provoke participatory responses. "Fake news," memes, or leaked data can be fed into sympathetic echo-chambers, and then spread further organically until they gain mainstream media attention. "Information laundering" dynamics can create a false impression of information diversity, while more insular niche networks play key roles in fostering extremist group identities and reinforcing biases. The ultimate target of many of today's information operations is the cognitive processes of individuals in society, and the willing participation of targeted sympathetic audiences plays a key role in amplifying what could otherwise remain fringe issues and narratives.

The discussion highlighted a number of unique challenges faced by democracies in confronting the threats emerging from the new information environment. Democracies rely on an informed citizenry capable of voting thoughtfully to represent their preferences. The freedom of expression is also regarded as a fundamental right, supporting this goal through the "marketplace of ideas." But the new informational environment demonstrates that sometimes more speech is no longer an adequate protection against false or divisive or hateful speech – speech forms that can in fact endanger civic education and threaten public civility. The use of similar techniques and platforms to influence domestic audiences by a wide range of actors, ranging from corporate advertising agencies and political campaigns to fringe extremist groups and foreign adversaries further challenges core democratic distinctions between "propaganda" and those forms of public persuasion long regarded as legitimate. The acknowledgement of these domestic challenges further complicates efforts to articulate clear norms regarding Internet freedom and online free expression on the international stage, where Western democracies have long opposed the efforts of non-democratic states to engage in norm-formation around unified concepts of national "information security" subsuming both the cybersecurity and Internet content components.
The group discussed the current state of efforts to address these problems, and debated the potential for more effective longer term solutions. While a great deal of attention has been paid to the

respective responsibilities of the private sector and government to implement effective terms of service, fix algorithms, or enforce regulations, many agreed that platform-/content- level solutions will likely never be cure-alls. Some participants were hopeful that the coming of age of a more tech-savvy digital native generation combined with long-term educational interventions could bolster societal resilience at the cognitive level making populations more resistant to disinformation and influence campaigns.

Panel 6: Roles of the Private Sector and Other Stakeholders

- How are cyber- and informational-conflict changing the nature of civilian cyberspace (including technical and governance structures of the Internet)? How significant are these changes in an historical perspective?
- To what extent are the security concerns of stakeholders at odds and where do they converge?
- How successful are current approaches in balancing values and interests? Are further innovations needed?

The private sector has a role to play both in maintaining cybersecurity and in mitigating the impact of information warfare. Whereas until the mid-2000s cybersecurity meant for the private sector to fend off cyber-criminals, today more and more state-sponsored attacks against private entities occupy the minds of those tasked with securing the sector's networks and information. While the financial industry has made great strides in the recent past to improve data security, considerable parts of the private sector lag behind. Nevertheless, the U.S. government has been remarkably reluctant to set and enforce regulatory standards for cybersecurity of non-state-owned networks, with four out of five legislative acts that do mandate cybersecurity standards dating back to the late 1990s; the 2005 Energy Policy Act, which set reliability standards for the electrical grid, remains the exception. Most of these consider cybersecurity as a component of privacy and only contain "soft regulations." Government-run networks, on the other hand, are fairly well regulated, so that, for instance, U.S. DoD contractors frequently encounter considerable hurdles.

Instead public-private partnerships have dominated the interactions between the private sector and government on cybersecurity, even when profit incentives do not necessarily align with the requirements of secure systems. While late Obama administration efforts focused on information sharing between the private sector and government, policy statements emphasized flexibility and technical specificity was scaled back. Congressional action remains unlikely.

Still, individual states have taken regulatory approaches to mandate cybersecurity standards. For instance, California mandates that private businesses take reasonable measures to ensure security, referencing the Center for Internet Security's Critical Security Controls as "a minimum level of information security that all organizations that collect or maintain personal information should meet." However, civil action on liability issues against the private sector is unlikely to produce groundbreaking results, because costs to negligent companies are fairly low, both in terms of litigation (cybersecurity insurance largely means litigation insurance) and stock-price recovery, and because litigation is structured to lead parties toward arbitration and not conclusive attribution of fault.

Even where the private sector, the government, and other stakeholders agree that cybersecurity must be improved, disagreement regularly erupts over how to deal with the inherent uncertainty of cyberspace. There is often poor mutual understanding of the problems and potential threats. Sometimes attackers even seem to understand networks better than their defenders. One participant described a typological classification of threats that could help in developing shared understandings of threats to be addressed. The proposed matrix would categorize threats by the types of uncertainty they exploited and the goals of the malicious actors who sought to exploit them. The matrix would then prescribe a certain kind of response against particular threat types. For instance, an actor who exploits the narrative uncertainty for mischief would require a different sort of response from an attacker that seeks to exploit uncertainty over identity for monetary gains. The former was presumably experienced by Miami Herald reporter Alex Harris following the school shooting in Parkland, FL in February of this year.[3]

The discussion addressed the need to rethink the standards of attribution for cybersecurity. Following the hacking of SONY, the U.S. government confidently pointed toward North Korea as the perpetrator only to be criticized for the degree of certainty the attribution presumed without being sufficiently transparent. Similarly, rather than soliciting a forceful response, the Russian hacking of DNC servers and election meddling led to infighting within the U.S. With the eventual winner of an election benefitting from foreign intervention, few incentives seem to have existed to secure the system and prevent future hacks.

In conclusion, the workshop ascertained that we might currently be experiencing "cybersecurity before Henry Ford," in that efforts are not yet scalable enough to ensure high security at low cost.

Panel 7: The Roles of Laws, Norms, and Limits in Constraining Cyber Anarchy

- What roles, if any, can international law, agreed upon rules, or emergent norms play in constraining cyber behavior and arms development?
- Are there any behaviors parties might agree should be off limits?
- What lessons can be learned from recent efforts or from experience in related domains?

Although various international organizations have, over the past two decades, devoted increasing resources to the development of a global cybersecurity agenda and norms for state and non-state conduct in cyberspace, so far, no comprehensive framework has emerged. Since 2010, the United National General Assembly, for instance, tasked subsequent Groups of Governmental Experts on Information Security (GGE) with carrying forward an international conversation on cybersecurity. The 2016/2017 GGE was to study "existing and potential threats in the sphere of information security" and measures to address them, including "norms, rules, and principles of responsible behavior of states, confidence-building measures, and capacity-building."

While previous GGEs had made headway in reaching common understandings and the 2016/2017 meeting also accomplished moderate progress in some areas, they failed to arrive at a consensus outcome report over how international law applies to the use of Information and Communication

[3] https://www.npr.org/2018/02/27/589279395/miami-herald-journalist-explains-how-a-hoax-tweet-affected-her-reporting-on-shoo

Technologies by states. A more promising route, according to some workshop participants, may lie in multi-stakeholder commissions, which would include the private sector and civil society actors and propose norms and strategies to governments. Like-minded countries should also pay attention to the G77, if they hope to eventually adopt a comprehensive international legal framework on cybersecurity. The void left by the world's cyber powers could also be filled with a spirited push by a group of small countries, which, even if not codified, could further the emergence of new customary law.

Discussion also drew on the work of the Tallinn Manual Process in examining how existing international legal principles apply to state activity in cyberspace. Here a clear distinction must be made between peacetime and wartime. During peacetime, the general prohibition of the use of force applies. When cyber-attacks create significant physical damage or otherwise threaten the survival of a state, for instance through economic damage, they are prohibited under Article 2(4) of the UN Charter. Coercive interference and intervention in the domestic affairs of another state is prohibited as well, as is the violation of another state's sovereignty and territorial integrity. The right to self-defense is also generally believed to apply in cyberspace. In war, international humanitarian law applies, which outlines, among other restraints, that an attack may only be directed against a military target, in targeting as well as in its effects. It appeared to many participants that Western states by and large subscribe to these constraints. However, they have been unwilling to engage in a debate about how international law might constrain specific activities and have been reluctant to even qualify the legality of enemy cyberattacks like "NotPetya," a result maybe attributable in part also to the complex interagency processes in many Western democracies. So far, most relevant governments have kept the threshold of Article 2(4) so high that they interpret cyber activity falling below it.

Russia and China have long considered existing international law ill-equipped to deal with information and communication technology and have promoted the need for a distinct treaty or code of conduct on the issue. While both countries agreed in 2013, as part of the 2012/2013 GGE, that international law is applicable to cyberspace, their resistance to clarification of the details of how it is applicable in 2017 can possibly be seen as indicating a residual reluctance to accept this applicability. Cuba, Russia, and China all objected to efforts to clarify the application of Article 51 of the UN Charter and the right to self-defense in cyberspace, with a Cuban statement on the disagreement stressing concern over legitimizing increasingly intense cyber conflict.

The failure of the GGE indicates a growing rift in approach, with Russia and China leading those states concerned more with an emphasis on sovereignty and domestic control over online flows of information for the sake of maintaining political stability. Restrictive domestic approaches to Internet control (often under the header of "information security") fit well with the more intergovernmental approach to global Internet governance also sought by these countries – as opposed by Western countries' focus on human rights and democratic freedoms in cyberspace and advocacy for the multi-stakeholder model of Internet governance. Russia has pursued a persistent diplomatic strategy along these lines since 1998, pushing for an international cyber treaty and later also leading blocs of countries promoting codes of conduct and proposed international Internet governance rule changes at the UN and ITU. Western countries have opposed these efforts, based on differences in perceived cyber threats (criminal or military, for example, vs. political), unresolved questions over verification and enforcement, the implicit inclusion of media and

Internet content as potential threats in these proposals (and perceived consequent legitimization of Internet censorship), and the diversion of attention from discussions over existing international law and how it applies to cyberspace, among other concerns.

Panel 8: Lessons Learned and Looking Ahead

- What lessons follow for the U.S. government and its allies concerning the further development of cyber- and informational-conflict capabilities, policies, and strategies?
- What lessons follow for ways to think about the dual use nature of cyberspace? What policies and processes can best accommodate the interests of multiple stakeholders and uphold democratic values while addressing national security priorities in cyberspace?

The final session brought together concluding thoughts on the workshop's topics and the state of the field. One theme running through the discussion focused on the state of government capabilities development and what more is needed, raising further questions about education and training, talent flow, and private sector-government relations. There is a clear need for more short- and long-term education and training programs - especially programs which provide understanding of both the policy and technical aspects of cybersecurity. These issues should be addressed in regard to elite talent development, and also in building greater awareness and resiliency in the general population.

Since a great deal of technical expertise resides in the private sector, participants discussed ways in which more career opportunity paths could be opened allowing top technical experts to rotate between government service and the private sector. Reciprocally, the need for more opportunities for academics and outside policy analysts to gain some insight into government cyber capabilities development and their repercussions was also addressed, with the suggestion that more such transparency and engagement would permit a more informed academic and policy discussion and ease existing tensions and distrust between communities.

In light of the limited degree of recent technology regulation, the group examined workable models of public-private partnerships that could be used to address existing problems and tensions. There was general agreement that this was particularly important in light of recent rifts following events such as the Snowden disclosures and the Apple-FBI case. While all stakeholders can agree that information technology is valuable to our lives and the economy, and that security is of vital importance, interests do not always appear to align on a more detailed level. But cooperative meetings and not-for-attribution discussions can play a valuable role in bridging these divides and fostering further collaboration.

As general observations regarding the state of the field, participants discussed the need for better analogies and greater attention to historical parallels. They also raised concerns about excessive hype regarding certain types of risk, in the absence of a more balanced public discussion. This could lead to threat inflation and to confusion as to the time scale within which solutions could best be sought. While short-term actions are in some cases critical, slower more patient actions and collaboration often can yield more appropriate long-term solutions.

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-750497