Conclusion: When Experience Speaks and Too Few Listen – Curating the Unlearned Lessons

Chris C. Demchak[1]
Francesca Spidalieri

The past decade has ushered the rise of a 'Cyber Westphalian,' increasingly conflictual world characterized by rising great power competition, which now has escalated into 'Great Systems Conflict'[2] across all digitally dependent societal domains. These struggles are occurring for, through, and enabled by cyberspace, and are now well in evidence globally. Yet, after ten years of experiments in creating organizations, strategies, policies, and offensive campaigns, consolidated democracies have either neglected or missed some valuable lessons. The essays in this special issue provide a broad overview of what was missed, ignored, mistaken, or simply not learned despite indications and experience. They also offer a way forward to tackle some of the more complex issues discussed. The unlearned lessons identified here range over issues of strategic approach, national scale and capacity, institutional change, and the socio-technical-economic system's framing of the cybered conflict challenge. The authors here—subject matter experts with considerable and well-recognized expertise—are concerned about what we collectively are failing to appreciate and act upon. They intend by these essays to inform future national strategies, policies, and institutions to ensure that these unlearned lessons do not turn into future strategic failures in a rising, deeply cybered, post-westernized, authoritarian world.

This final essay offers a brief overview of these critical unlearned lessons.

With degrees in engineering, economics, and comparative complex organization systems/political science, **Dr. Chris C. Demchak** is Grace Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber Innovation Policy Institute, U.S. Naval War College. In publications and current research on cyberspace as a global, insecure, complex, conflict-prone "substrate," Dr. Demchak takes a socio-technical-economic systems approach to comparative institutional evolution with emerging technologies, adversaries' cyber/AI/ML campaigns, virtual wargaming for strategic/organizational learning, and regional/national/enterprise-wide resilience against complex systems surprise. Her manuscripts in progress are "Cyber Westphalia: States, Great Systems Conflict, and Collective Resilience" and "Cyber Commands: Organizing for Cybered Great Systems Conflict."

Strategy Unlearned Lessons

For starters, neglect of strategic lessons in a rapidly evolving and increasingly conflictual cybered world is particularly troubling. Today's larger powers find themselves in a growing struggle over global governance, pitting a democratic model that endorses the rule of law against an authoritarian alternative driven by centralized social control and arbitrary use of power. In this struggle over the digitized world order, cyber insecurity has emerged as both a sovereign issue and an international challenge prompting a multiplicity of discussions at the United Nations (UN) and in other international fora about internet governance and how to constrain harmful state behavior in cyberspace. Unfortunately, after almost twenty years of discussions and negotiations on the threats of malicious state activity in cyberspace and on the relevance of international law related to conflict in and through cyberspace, the diplomats and international lawyers of consolidated democracies have succeeded in negotiating only *non-binding* norms on responsible state behavior in cyberspace published in much publicized high-level UN reports.[3] In all these negotiations, they ignored events over the last two decades in which states freely used cyber tools for their political, economic, and military objectives, often in violation of the same norms they had underwritten and largely without any negative consequences. The paucity of concrete effects of these paper norms demonstrated a widely unlearned lesson about precisely what international binding law is, how it is actually created, and how it differentiates from voluntary norms, in particular, that norms only become legally binding when they are widely and consistently observed and enforced by states themselves. (Catherine Lotrionte, pp. 23-31) As a sad result, the two decades of discussions contributed more to the theatric appearance, but not the reality, of a cybered, safe, stable, and rule-bound global system.

Francesca Spidalieri is an Adjunct Professor for Cyber Policy at the University of Maryland's School of Public Policy and works as a cybersecurity consultant for Hathaway Global Strategies, LLC. She is also the Co-Principal Investigator for the Cyber Readiness Index 2.0 project at the Potomac Institute for Policy Studies, and the Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University. In addition, Francesca serves as a cybersecurity subject-matter expert for the World Bank, the Global Forum on Cyber Expertise, the UN International Telecommunications Union, the EU CyberNet, and several other research institutes in Europe. Her academic research and publications have focused on cyber leadership development, cyber risk management, digital transformation, and national cyber preparedness and resilience. She lectures regularly at cyber-related events in the United States and Europe and contributes to journal articles and other publications on cybersecurity matters affecting countries and organizations worldwide.

Equally unlearned among the democratic like-minded communities is that states – and only states, not commercial firms, or civil groups – have the capacity, incentive, and legitimacy to negotiate with other states to find a common understanding and agreement on how to ensure a more stable, open, and interoperable cyberspace. Despite the demand from a wide range of civil society and private-sector actors for a role in international public policy for cyberspace, cybered conflict and diplomacy remain the purview of states. In this contest, states have a legitimate right and assumed obligation to defend their society and citizens. (Jim Lewis, pp. 33-39) Only when major powers agree to observe these norms, start to publicly attribute malicious cyber activity to other states, and invoke international law in their responses, these norms may actually develop into legally binding law over time.

There are other strategic-level lessons left unlearned on the table. Major lessons about the rising, biggest, and most formidable adversary yet – an increasingly authoritarian China – have taken a decade to be recognized, let alone acted upon. As the era of a dominant liberal international system declines with the rise of authoritarian-leaning states and Great Systems Conflict, the unlearned lesson was and remains that simply engaging with China will never deliver the hoped-for economic development and progressive normalization of society. Despite several decades of this Westernized politesse, China's government has not evolved towards an "autocracy-lite" regime that could play a more constructive and stabilizing role globally, as was expected by a wide variety of Western experts, economists, commercial leaders, and policymakers. The markedly illiberal turn that China has taken in the last decade came with demands for the international order to be modified to accommodate its emergence as a powerful strategic competitor and major global power. The seemingly surprised democracies continue to

suffer not from a lack of knowledge but from a lack of cultural and historical context and a failure of imagination. Cloaked by a westernized "end of history" mindset blocking an accurate perception of reality, China has been free to turn Western dominance of information communication technologies (ICTs) into a significant vulnerability. In contrast, its regime has reinforced its domestic hold on power and shaped the international climate and some standard-setting bodies to favor its interests.

Even more "uncomfortable" lessons are yet to be learned. First, given the latitude accorded to China over the past two decades, Western power must now yield to pragmatism. Second, Chinese technology, like China itself, is here to stay and cannot be totally excluded from Western markets and, third, some of those technologies will inevitably be superior to those developed in consolidated democracies. Fourth, a US global leadership role is no longer assured as China will be a major economic player for the rest of the century. (Nigel Inkster, pp. 41-48) Unlearned strategic lessons about China have permanently changed the future for democratic like-minded nations who refused to see them.

Another pragmatic lesson is one that must be relearned from the Cold War – namely, that technology can offer some common ground between peer cyber competitors on which to build mutual trust and a common framework. Achieving cyber stability among cyber competitors is not predicated on congruence across all domains of cyber engagement but requires finding at least some areas of common interest or agreement and then engaging in confidence-building measures. This is a lesson learned during the Cold War, in which small science and technology teams from the US and the former USSR worked on joint projects provided these connections, enabling bilateral understandings despite hostility. This approach requires relearning that it can be more productive to narrow the problem-solving efforts to common and yet neutral problems to find plausible solutions that accommodate all positions and prevent potential escalation. (Chris Spirito, pp. 51-56) As the world increasingly reflects Chinese interests and priorities, learning this lesson can help open more pragmatic options to avoid constant escalation on the cybered conflict spectrum of the already emergent Great Systems Conflict.

National Capacity Unlearned Lessons

Moving from the strategic level to a more national or strategic-operational level, several lessons with implications for the pursuit of capabilities have yet to be learned. The first is that a functioning state must maintain its monopoly of force, which is critical for national viability in a conflictual cybered world. For most of the past decade, the bulk of the westernized democracies publicly disavowed offensive cyber capabilities save in their militaries to defend solely military forces. Yet, the lesson of a hostile cybered world is that a viable state cannot renounce its offensive cyber capabilities any more than it can refuse to defend the nation physically. Offense and defense in cyberspace are two sides of the same coin, and both are required, along with systemic cyber resilience, for robust cyber power.[4] For a state to

have a competitive strategic advantage in cyberspace, become more resilient, and be able to effectively influence or convince others in international discussions or negotiations, it will have to learn to harness the right (and sufficient) talent, teams of experts, and competent senior leaders; fund national cyber resilience efforts with intent; and be willing to devote time and resources to "continuous, expensive, offense-informed, real-world trial-and-error experiments." (Sandro Gaycken, pp. 61-73)

Another strategic-operational lesson not fully learned by democratic states is the rising necessity for allies to work together in all aspects of national cyber security. The community of consolidated democracies will be an enduring minority of states, each facing a huge adversary like China and its fellow travelers such as a resurgent and aggressive Russia. Only with collective strategic and operational narratives and capacities can they defend their future and ensure the survival of democracy. For almost four generations, this lesson has been especially neglected in the US – the largest, wealthiest, and strongest among consolidated democracies. It has historically placed too little emphasis on the importance of such collaboratively developed strategic and operational narratives and decisions. In the Great Systems Conflict era, working with allies as peers is a critical, strategic-operational necessity. In a deeply cybered nation, whose entire socio-technical-economic system is struggling with massive onslaughts from state-sponsored attackers and criminals, defending alone leads to strategic and operational defeat over time (Ed Cardon, pp. 75-80). There are many other unlearned lessons about what contributions allies, team partners, private sector entities, and other organizations collectively operating in complex challenges can provide that would otherwise be unavailable, and these lessons need to be learned institutionally and strategically very soon. (TJ White, pp. 83-91)

Furthermore, a related unlearned lesson for the increasingly conflictual cybered world is that the expectations about some otherwise solid allies' help will have to be strongly nuanced according to their particular geopolitical and capability challenges. Some smaller states/partners cannot confront China in the way that only the US has the capacity to do. Their survival depends on a pragmatic balance between the two. Singapore is one such state – a small but highly connected island nation, considered a regional thought leader in cybersecurity. Despite having been both the target and the launching pad of significant cyber attacks (likely emanating from China), Singapore and similar neighboring ASEAN nations have often chosen not to publicly attribute such state-sponsored cyber incidents, carry out countermeasures, or showcase offensive capabilities. These choices were made to protect the safety of their intelligence sources, prevent escalation, or avoid harming their vital trade relations with China, as well as other pressing reasons. The risks of cyber conflict or adverse effects on trade for this highly connected nation are arguably too great for that tiny state to absorb, even if they are—in terms of values and longer-term preferences—clearly aligned with other westernized democracies. (Ben Ang, pp. 93-99) It is the example of such allies that

can help the US to learn to be sensitive to the circumstances of its smaller and yet critical geo-strategically placed allies.

Another small but very capable partner with lessons to offer the US and its larger allies is Israel. Despite its small size, modest budgets, and limited natural resources, Israel has used a small nation's advantages in information sharing and coordinated policies to develop a comprehensive, whole-of-government, and whole-of-society national cyber security strategy and policies. It has succeeded in centralizing authority and resources required for national cyber defense, developing cybersecurity operational capabilities that allow for quick decisions and the ability to change directions when needed at relatively short notice, and fostering a thriving cybersecurity ecosystem and industry. The lessons behind this success have been available for some time but not learned by its largest ally. Indeed, the tendency among US policy makers has been to assume most of Israel's lessons are not scalable to a nation the size of the US. Yet, many of the ignored lessons involve seeing Israel as a pilot project to develop more operational capabilities for whom scaling up is not the lesson. Rather, these lessons involve small-scale capabilities, irrespective of the size of the nation, such as assembling elite (non-military) groups of national cyber specialists ("cyber commandos") to tackle high-end techno-operational cyber-attacks. Another scale-indifferent lesson would be developing a more deterring or attacker-oriented response to cyber threats. Rather than narrowly using the U.S. Cyber Command (USCYBERCOM) or the National Security Agency (NSA) to react or focusing federal agency actions mainly on attribution (or naming and shaming, indictments, expulsions, demarche, designations, and sanctions), the US should learn the whole-of-society defense lesson of Israel. It should be developing nonmilitary "small elite teams" to answer the nationally relevant and exceptionally difficult techno-operational questions found in hunting state-level adversaries across society. Above all, the lesson from Israel is to provide this civilian commando team with top analysts and access to relevant data and tools, a "shielding bubble" protecting them from non-essential political and managerial interference, and to keep them small to maintain their agility. (Eviatar Matania and Lior Yoffe, pp. 101-109).

Policy and Organization Unlearned Lessons

Moving from the national or strategic operational level to the institutional level, for federal agencies or departments in the US, the lesson of importance and persistence was learned through cybered conflict, but only belatedly. It has taken a long time for a large power like the US to learn that perseverance in confronting an enemy's cyberspace is necessary to effectively deter, constrain, thwart, and frustrate adversaries over time, preferably before they can achieve cumulative strategic effects. The concepts of "persistent engagement" and "defend forward" were first introduced in 2018 by USCYBERCOM and then incorporated by the U.S. Department of Defense (DoD) into their new cyber strategy. These approaches challenged the previously dominant assumptions and prescriptions of deterrence theory. Wheth-

er the state responds or not, the new presumption is that authoritarian states and non-state actors will always continue to conduct malicious cyber activities to protect their regimes, undermine political cohesion in the West, delegitimize democratic institutions, and reduce the economic, political, and military advantages of the US and its allies, etc. Before and after the publication of these documents, the evidence was clear that cyberspace campaigns against the US and its allies were continuous and ongoing, and that adversaries would persist given the low cost of entry, anonymity, non-timely attribution, ambiguous redlines, and the number of pervasive system vulnerabilities to exploit. Therefore, in 2018, the US began to learn the lesson that to compete and persevere, one requires persistence in engaging and seizing the initiative and in defending forward (outside system boundaries and as close as practicable to the source of malicious activity), not acting with restraint and episodic responses, and in anticipating rather than simply reacting or threatening future actions. (Emily Goldman, pp. 113-118) Ironically, this lesson resembles the constant engagement of naval forces during the Cold War, suggesting – not for the first time – the similarity of cyberspace to the ocean for a submarine and, thus, leading to the implication that this lesson is really just being relearned. However, many of our more advanced allies have yet to learn this lesson for even the first time.

If one is to engage persistently, then how is one to gauge effectiveness of the operations? Metrics – more precisely the lack thereof – constitute the soul of a further difficult to learn lesson, specifically for institutions trying to conduct defensive operations. Leaders need to comprehend the wider scale of the threats to balance all these responses. Resilience, competitiveness, and effectiveness rest on having an accurate vision of the scale and scope of cyber threats. Clear, objective, and repeatable metrics can help measure the success and effectiveness of cyber-related policies and initiatives in the deceptive and opaque cybered world. This lesson requires an emphasis on developing and employing metrics to measure the real impact of cybersecurity initiatives, such as whether efforts have effectively reduced the number of intrusions on critical systems or the impact of cyber-attacks. Such metrics are as yet unavailable. Agency, corporation, and state-level policies and operations are in effect shooting in the dark about whether procurement policies and acquisition rules appropriately incorporate cybersecurity standards and cyber resilience requirements; or where and how the private sector has adopted appropriate security measures and best practices that embody internationally recognized standards of care (e.g., encryption, MFA, patching, auditing, liability regime). Many questions are unanswerable without objective metrics. These include questions of how cyber issues impact citizens' security, privacy, and civil liberties; whether they have adopted cyber hygiene best practices; and whether international cooperation against cybercrime and cyber-enabled crimes has minimized the impact of serious attacks on society or reduced the number of safe havens for criminals. Without valid metrics, it is difficult to formulate informed and coherent policy or operations, let alone learn from the lessons of the past. (Harvey Rishkof, pp. 121-126).

Persistent engagement without metrics to gauge effectiveness can also lead to policy tunnel vision where some tools are repeatedly used, and others ignored. As one of the most connected ICT-dependent countries in the world, the US is at a distinct disadvantage if it limits responses to largely military-borne cyber operations and minimizes other diplomatic, information, military, and economic ("DIME") instruments of national power. The US needs to learn the lesson of adopting a smart and consistent use of all the DIME tools and resources already at its disposal to prevent and respond to future aggressions in, through, and enabled by cyberspace, while also strengthening partnerships and alliances across Western democracies and other global regions. (Michael Klipstein and Pablo Breuer, pp. 129-135)

Another lesson about not leaving options on the table in operations and policies concerns effectively integrating the inevitably significant role of private sector actors in a digitally conflictual era. They produced the underlying shoddy cyber substrate, and they now develop, operate, produce from, expand, maintain, and advance it technologically. Their operations are often on the front line of adversarial campaigns, and they are used as pawns in economic warfare. Their enterprises are targets of widespread theft of intellectual property to achieve later market control, or the victims of takeovers, investments, bribery, or blackmail. They are unable to force cyberspace to be more stable and secure when dealing with ruthless authoritarian states. However, the unlearned lesson is that they (and their interests) certainly have a role as advisors, implementors, and innovators to inform the international and collective allied operational negotiations conducted by states to assure national defense. (Andrea Little Limbago, pp. 137-149)

Socio-Technical-Economic Systems (STES) Unlearned Lessons

Having the private sector inside the defense tent does not mean better outcomes if they and the governments they support miss this another lesson about the integrated relationship between the underlying cyberspace and emerging new technologies and their increasing criticality across digitized societies: what infects the parent infects the child. Reaching across the strategic, national, and institutional levels, technological integration of a nation's socio-technical-economic systems (STES) strongly influences its basic load of cyber vulnerabilities that are passed on to the new emerging technologies. These new technologies are built on, meant to be embedded in, and will operate through the underlying cyberspace. The fundamental inability to secure that cyberspace is costing consolidated democracies 1-2% of their GDP annually[5] and is responsible for accelerating the rise of China as the chief adversary of the previously dominant liberal rule of law over the global system. The same security-averse tendencies that marked the computer vendors, internet promoters, and then paid cyber defenders of the original and shoddy cyberspace substrate are now leaving vulnerable the entire life cycle of emerging technologies, from artificial intelligence to quantum and so on. Unless and until that underlying cyberspace jumble is transformed into something securable, defensible, and resilient, emerging technologies built on it will remain vulnerable.

The apple does not fall far from the tree, and the tree must be transformed for the surrounding society to survive in the coming more authoritarian world. (Chris Demchak, pp. 153-160)

A particularly difficult and clearly unlearned lesson about national socio-technical-economic systems is how to prepare for the inevitability of failures in large complex digital systems. Given the level of integration across digitized societies, smaller failures can cascade into disasters, especially those that adversaries could start or help along. What might be called for is old-fashioned "prudence" in assuring ubiquitous alternatives and functional backups that can be used when – not if – complex catastrophic events occur. But backups must be regularly updated, tested, and maintained, not assumed to be available. Given the numerous problems of today's cyberspace (including unethically designed embedded systems, unmanaged connectivity, and failure by design), the most important unlearned lesson boils down to the imperative that (analog) backup alternatives must not be let to wither. The only way to protect and thereby be systemically resilient as a nation is to have healthy and available analog equivalents providing the same services as the cybered functions on which so much relies. (Dan Geer, pp. 163-173)

Following on that systemic argument for an entire nation is another as-yet unlearned lesson: keeping less complex, opaque, and potentially unmanageable systems on hand to be able to function systemically when the adversary imposes surprise. This lesson is particularly critical for military forces like the U.S. Navy. Four questions underlie this lesson, and these must be answered before the service can be assured that it is resilient to the kinds of intrusions, disruptions, and even deception that the adversary China and any fellow travelers will attempt at scale, en masse, and repeatedly. The four questions on cybersecurity concern tradeoffs between security versus efficiency and convenience, the need for a less digitized reserve, the possibility of enforced autonomous systems use, and the obstacles to fleet design that achieves the Navy's distributed maritime operations (DMO) concept. The Navy must answer these questions by examining its systems, procedures, doctrine, and force designs, lest the cyber vulnerabilities mean losing a conflict with a technological near-peer like China. (Sam Tangredi, pp.175-179)

A deeper unlearned lesson about democratic socio-technical-economic systems' dependence on the cyberspace substrate requires recasting 'content' or data in cyberspace as infrastructure that needs protection and resilience as much as physical installations. Consolidated democracies must learn that data integrity, along with confidentiality and availability, must be given the same attention (and appropriate resources) as physical infrastructure. Content should not be conceptually separated from cyber security in discussions, policy, or defense operations. This lesson is particularly critical as the world heightens reliance on artificial intelligence (AI) and machine learning (ML) algorithms. These emerging technologies require large volumes of training data and are currently largely developed with little attention to cyber security during their lifecycle. (Sean Kanuck, pp. 181-190)

Furthermore, content rides among countries on international networks, and another lesson yet to be absorbed concerns the abuse of this complex connectivity by adversaries of democratic nations. Political and administrative communities in most established democracies rarely have any technical training or in-depth understanding of cyber threats to their networked infrastructures. They have not been aided by technical advisors who have been for two decades slow to perceive or unwilling to call attention to the threats buried in the insecurity of the same networks. Late in the last decade – in 2018 precisely, some senior leaders of national security communities of the US and other allied nations were informed about the increasing threat from state-sponsored hijacks by their major adversary – China – and other state-level bad actors. By then, many technologists across the network defense communities were willing to acknowledge awareness of these campaigns. Nonetheless, only a few consolidated democracies are attempting to counter these attacks with limited responses, likely too focused only on one actor – China – and only some of its corporate bad actors. These attacks have continued, indicating this lesson has yet to be learned. (Yuval Shavitt and Chris Demchak, pp. 193-205)

Finally, one surprising, unlearned lesson concerns the paucity of government support for cyber insurance. It is not an overstatement to attribute much of the stability in prosperity in the US to the rise of affordable and regulated insurance across sectors and products. Yet cyber insurance is currently burdensome to obtain, increasingly expensive, too narrow in coverage, and too focused on firms with large budgets. This is an unlearned lesson in the US even though there is already a successful model of a solution from broadly similar circumstances. The FDIC is a nearly century-old insurance scheme enacted to resolve similar and possibly catastrophic risks to the US banking system in the early 20th century. Like cyber incidents today, failures then (and now) in the banking system could (and did) quickly cascade to harm the entire national socio-technical-economic system and beyond. Like cyber today, medium and smaller firms had no chance of surviving without government help. A national cyber insurance scheme could provide multiple benefits across the national cyber substrate, including helping small and medium firms – the bulk of the internal economic activity and lifeblood of the national STES – learn better how to choose their technologies, operate them more safely, and be more resilient to the inevitable disruptions and failures. In short, governments defend their societies, and that should include creating public insurance for cyber just as they would nurture any other kind of societal resilience across sectors, locations, and threats. (John Harvey, pp. 207-214)

Concluding Remarks

By our account, there are at least 20 yet-to-be-learned lessons forming a converging picture of what has escaped our vigilance over the past ten or more years. From a systemic point of view, especially in using the framing of socio-technical-economic systems, the lessons form an overarching meta-lesson about systemic resilience and forward disruption as key

components of national cyber power. The expert views discussed here clearly indicate that governments have a central role to play in building the nation's cyber resilience. Still, all sectors, whether private or public, need to be inside the cyber defense tent. These experts have pointed out several yet-to-be-learned lessons across cyber-related disciplines, from the need to use international law appropriately and negotiate at the state level intelligently with knowledge of the adversary and agilely on some topics but persistently standing firm on others with the necessary defense capabilities, service funding, and tailored teams, to absorbing the help and experience of allies big and small, and finally to rethinking the connectivity of and structure, technology, indemnification, and nondigitized reserves of the whole. The big picture painted by our experts suggests a fragmented narrative has blinded national political, economic, and technological leaders for a decade or more.

Unfortunately, the pock-marked and stubbornly dominant American zeitgeist that views national power from the triumphal twentieth-century lens of a remaining, untouchable, and immutable superpower, unfortunately, extended the same broken, unsystematic definitions to cyberspace. For over three decades of cyberspace's maturity, self-evident lessons have been obscured from the US and key democratic allies' views. By 2010, cyberspace was clearly identified by the US and several allies as a first-tier threat, yet the self-evident reality still struggled to be seen. Even top-tier master's degree schools feeding future leaders to senior agencies and corporations were largely oblivious in their curriculum to the rising threats of cybered aggressive state adversaries and crime.[6]

Now, over a decade later, after cyberspace was declared a top-tier threat by the US and several key allies, several key lessons remain unlearned. These lessons should have been obvious from the outset. Cyber power rests on the capabilities of a state to engage in legal forward disruption, but it also critically depends on the systemic resilience of that nation's socio-technical-economic system. And states smaller than China will eventually fall to its relentless pursuit to be the central global actor in international economic and technological interactions, unless these states gather to form a collective peer to jointly defend their collective technical and economic futures through a cyber operational resilience alliance (CORA). If they fight alone, China's rise, although bumpy here and there, is likely to reward the authoritarian state with the first seat among nations politically and inevitably socially, a slow form of vassalization of both democratic and non-democratic nations.

Allies in cooperation and joint operations, the central organizing role of democratic governments with private sector support, securable emerging technologies, analog backups and reserve forces, capable agile red teams focused forward, even public cyber insurance – all these unlearned lessons and more have been identified in this issue. And our experts explained the lessons' criticality to national power, especially in the various contributions to the cyber resilience of the nation. There are, of course, more unlearned lessons than those described here. However, if each of the democratic nations' public and private leaders act

collectively on the lessons outlined here, the next issue on unlearned lessons might be much shorter. In that latter ideal case, a future special edition of *The Cyber Defense Review* would examine how consolidated democracies collectively succeeded at creating robust cyber power through national cyber resilience. Instead of schooling leaders on what they have not learned, the next set of authors could be offering a how-to manual on prosperity, security, and cooperation in a cybered world. Each of these essays implies that ten years is long enough for neglect and handing advantages to the rising peer adversary. One must act on these lessons before the options they offer today wither away. Current trends do not favor the democracies in the Great Systems Conflict era. Time has a way of running out for those who refuse to learn.

NOTES

1. All ideas in this essay are solely those of the authors and do not reflect the positions of any element of the US government.
2. Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *Cyber Defense Review* 6, no. 2 (Spring 2021).
3. For example, the consensus reports adopted by the UN Group of Governmental Experts (UN GGE) and the UN Open-Ended Working Group (OEWG) in 2021.
4. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, Georgia, USA: University of Georgia Press, 2011).
5. Melissa Hathaway, "Interview on Tiktok, Wechat, and U.S.-China Decoupling with Melissa Hathaway and Gary Rieschel," interview by Gary Rieschel, *Expert Discussion*, August 13, 2020, https://www.ncuscr.org/event/tik-tok-wechat-us-china-decoupling/video.
6. Francesca Spidalieri, "One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," *Pell Center for International Relations and Public Policies*, March 2013, https://salve.edu/sites/default/files/files-field/documents/pell_center_one_leader_time_13.pdf.