Tallying Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020

Chris C. Demchak
Francesca Spidalieri

The world is now ten years into the age of overt cybered[1] conflict. The "Cyber Westphalian" world is well past infancy, and the newly conflictual world arena faces emerging great power competition across all domains. It is time to tally up the learning.

These essays engage that challenge with a twist. They look at what was missed, ignored, mistaken, or simply not learned despite the indicators and experience. This issue reflects most of a conversation held at the U.S. Naval War College in November 2020 where a small group of senior cyber and security practitioners and scholars met for three half-days to share and discuss the lessons of the first decade of cybered conflict. Included among the attendees were former commanders of the various U.S. cyber commands, as well as senior scholars of international relations with considerable cyber research experience. Others averaged a decade or several in involvement with and study of cyberspace, cybered conflict, and cyber campaigns.

1 "Cybered" is an adjective indicating the spectrum of effects from cyberspace as it acts, enables, or operates through the wider socio-technical-systems of a modern society. Developed first in 2011 as part of the term "cybered conflict," it was meant to indicate a broader range of conflict beyond the networks and struggles between states and groups ranging from peace to war. Today, while the term "cyber" used alone encompasses the universe of artifacts and effects associated with the rising thoroughly digitized world, the term "cybered" is still necessary to indicate effects beyond digitization – a more comprehensive view. One might say the 'digitized world' is a more neutral and even innocent framing of what has happened with the onset of the current era, while the "cybered world" clearly points to the rise of great power and now Great Systems Conflict. See Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (March 1 2011). Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).

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."

Unlike other workshops, the charge was not to list successes but to uncover failures to learn across the US and its democratic allies. The meeting, titled "'Entre Nous – Blunt Lessons of Cyber Strategy and Stability," focused on identifying the overlooked, underappreciated, or novel strategic and organizing lessons that still needed to be – or never had been – recognized. The workshop concluded with discussions of what was needed to have these unlearned lessons recognized and implemented across Western democracies going forward. The organizing hosts were the NWC's Hopper Chair of Cyber Security (Chris Demchak) and Leidos Chair of Future Warfare Studies (Sam Tangredi), both part of the Cyber and Innovation Policy Institute, and the co-hosts were the European School of Management's Digital Society Institute Director (Sandro Gaycken) and the Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center Research Director (Lior Tabansky). Together, the organizers sought to change up the discussion to stimulate a wider view of what was missed over an incredible ten years of learning about cyber conflict and the rising of the digitized Great Systems Conflict in the waning Westernized global system of a post-Cold War unipolar world.

The results of the discussion's attendees and several additional well-known cyber experts are captured in this collection of essays on unlearned lessons over the past decade. There are four sections that begin with the highest level of generality (strategy and key actors), move to more national capacity issues, then to policy and organizational oversights, and finally roll broadly to the systemic questions transcending all levels. The sections are titled accordingly: Unlearned Strategy Lessons, National Capacity Lessons, Policy and Organizational Lessons, and Socio-Technical-Economic Systems (STES) Lessons. Each section presents three to five distinct discussions of one or more lessons unlearned or missed and the way forward.

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.

The arguments are based on the experience, research, and observations of these senior cyber and national security experts.

The purpose is to identify the shortcomings in as crisp a manner as possible to stimulate critical thinking in the readers and, one hopes, direct action on the part of those involved in policy, strategy, and leadership positions. Therefore, the essays are short. While the collection is equally intended for the use of scholars, practitioners, and students, it is not meant to be a deeply academic aggregate arguing with other publications, scholars, or pundits. Rather, its central purpose is to bring forward these lessons in as brief and yet persuasive a form as possible to make them useful for today's policy, strategy, or classroom discussions.

After ten years of experiments in creating organizations, strategies, policies, and campaigns for, through, and enabled by cyberspace, it is important to know what of value in lessons to be learned has nonetheless been neglected or missed in reality. The fervent hope of these authors, the editors, and those who attended that discussion twelve months ago is that this collection will interest security studies communities, strategic analysts, cybersecurity specialists, and service members as well as upper-division students and generalists. It will be accessible and yet have enough depth to guide education and stimulate curiosity and research questions. Some essays will contain some controversial observations and corresponding conclusions. These need to be refracted through future national strategies, policies, and institutional lenses for the future lest the unlearned lessons contribute to hard, painful lessons in strategic failures in the rising deeply cybered, post-Westernized, authoritarian world.

No edition of any journal can occur without the considerable help of those who made it possible. In our case, that support begins with the germinating workshop itself. First and foremost, the generous support

and insightful thinking of the U.S. Naval War College's Leidos Chair of Future War Studies, Dr. Sam Tangredi, enhanced the discussion and focus throughout the meeting. Our allied co-hosts, Dr. Sandro Geycken of the European School of Management's Digital Society Institute (ESMT/DSI) and Dr. Lior Tabansky of Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center (BICRC), provided the necessary alternative views to widen the thinking of the attendees and the offerings in this special issue. That support is and was deeply appreciated and will be sought – along with the presence of these eminent scholars – in future meetings. Beyond the academics and the practitioners are the critical staff members whose innovative and energetic support turned yet another virtual workshop into one that felt "intimate" and collegial, according to one senior attendee. Key members were Andrea Gonzales and David Bolender, both of whom are now a part of the ongoing team for all future Hopper-Leidos Chairs' Strategic Dialogues.

This special issue is not the last to address what a decade of experimentation might have missed or what ten years of evolution might have gotten wrong. Yet, it is an unusual issue in that everyone participating in the collection has been in the cyber security community with a close-up view the entire time. A number of them were in the position to make or debate important decisions. For many, the lessons identified as unlearned are quite close to personal experiences, and their professional concerns that we do not continue to neglect to learn is deeply held. We all hope this issue will spark reconsideration, open up some debate, and help reveal alternative future paths. We only have one world, and we are moving very fast toward its next and already more conflictual iteration. It is time to make sure we are noting the missteps before it is too late to correct them in the future.

NOTES

Chris C. Demchak, "Achieving Systemic Resilience in a Great Systems Conflict Era," *The Cyber Defense Review* 6, no. 2 (Spring 2021).

Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (March 1, 2011): 31-62.