Military Cyber Affairs

Volume 3 | Issue 2 Article 1

December 2018

Introduction to MCA Issue, “Systemic Cyber Defense"

Chris C. Demchak
chris.demchak@usnwc.edu

Introduction to MCA Issue, “Systemic Cyber Defense"

Cover Page Footnote

The views and ideas expressed here are the authors alone and do not represent those of the U.S. Government, the Department of Defense, U.S. Navy, or U.S. Naval War College.

Erratum

Notes added to reflect the recent transition from the Center for Cyber Conflict Studies into the Cyber and Innovation Policy Institute.

Introduction to MCA Issue, "Systemic Cyber Defense"[1]

Chris C. Demchak, Issue Editor[2]
Benjamin Schechter, Assistant Editor[3]

The study of cybersecurity is fractured by differing theories, concepts, and perspectives on behaviors and events, and the consequences are fractured recommendations and policies. What is critically needed now is a systemic picture of the emerging world and the longer-term security implications for westernized democracies. This issue constitutes the proceedings from a meeting of senior national and international subject matter experts from academia, industry, and government focused across two days of deliberations on closing the circle from broad challenges to implementing solutions. On May 1st and 2nd, 2018, the U.S. Naval War College's Center for Cyber Conflict Studies[4] hosted its 6th Biennial Cyber Workshop entitled"*: Integrating Economics, Information, Innovation, and Operationalization.*" The meeting's objective was to integrate disparate themes, data, and arguments about cybersecurity. To ensure a comprehensive, international perspective on what should be done, the discussion was co-sponsored by the European School of Management and Technology's Digital Society Institute, and participants were personally invited from allied national security and academic institutions.

Assembled in this issue are the written contributions to the workshop. The group of experts drew from themes of systemic economic maladaptation and losses, declining western global innovation dominance, and a diminishing US-led international civil society into implications for militaries tasked with defending the Nation and allies in a deeply cybered, post-western world.

[1] The views and ideas expressed here are the authors alone and do not represent those of the U.S. Government, the Department of Defense, U.S. Navy, or U.S. Naval War College.

[2] Dr. Chris C. Demchak is the RDML Grace M. Hopper Chair of Cyber Security in the Strategic and Operational Research Department at the U.S. Naval War College.

[3] Mr. Benjamin Schechter is a Research Associate in the Strategic and Operational Research Department at the U.S. Naval War College.

[4] As of this publication, Center for Cyber Conflict Studies (C3S) has transitioned into the Cyber and Innovation Policy Institute (CIPI). The change builds on this and prior work by C3S in an expanded and strengthened community of cyber researchers at the U.S. Naval War College.

Key conclusions from the meeting emphasized the need for new models of defense and economic thinking to prepare the defense and commercial communities for the reality of an antagonistic, overwhelmingly larger, cybered authoritarian world. The following captures the main observations.

First, without the creation of new models, recognizing the criticality of private sector participation in defense, states will continue to be at risk. There is currently no narrative or encouragement for private sector leaders to acknowledge the systemic threats their organizations face, let alone the existential threats to their whole society. The lack of an inclusive national digital policy is the result of twenty years of stagnation; complacency about the security of a shoddily constructed internet allowed everything to be connected without regard to possible deleterious consequences. In contrast, major adversaries are today engaged in a great deal of digital policy innovation, domestic regulatory experimentation, and international IT market shaping to advance their economies, strengthen their international leverage, and prepare the future cyber-physical battlefield to their advantage. In democratic civil societies, however, segmentation of governmental cyber defense efforts and fragmentation of government support for systemic innovations have been allowed to happen without foresight and direction. The results are national digital economic strategies in that do not incorporate defense concepts or consider them as critical as product development or market growth for national well-being and security. Neither incentives nor regulations have ensured secure, interrogatable designs and algorithmic transparency as baseline production requirements for current and future IT systems.

Second, the critical widespread national investments in secure technologies as a public good have been allowed to wither under a misplaced presumption that the commercial market innovation will provide adequate investments to meet both private and public systemic needs. System-wide disaster resilience and recovery has only been shallowly discussed by the government and in the private sector, with limited requirements for backups and only vague evidence of effective resilience. There is an assumption that outside sources will provide mitigation and recovery irrespective of the scale of the disruption. Furthermore, the effects of weakened alliance systems and anti-globalization politics on the ability of westernized democratic states to organize and mobilize collective resource for cyber defenses in the future are not adequately studied.

Third, in contrast, the major rising adversary – China – has been routinely mischaracterized by both the defense and commercial sectors. Much can be learned from adversaries if one perceives them accurately. China is a strategic opportunist, not fundamentally hostile as yet. Its extraordinary economic successes are in part due to western democracies' unwillingness to enforce WTO requirements or punish bad behaviors across cyberspace. The economic and ultimately defense blindness of these democracies is largely due to their own shared, flawed set of assumptions that the global international economic systems would inevitably drive China to open its markets and comply with international norms and laws. These assumptions have not played out, as China's autocratic political system naturally links the government with its IT capital goods industry. The resulting cooperation in the exploitation of international markets creates a coherent and winning combination of resources, strategic goals, coordinated large-scale efforts, and providing resilience (when needed) as a formidable, large scale, nearly ubiquitous economic and security challenge democratic states. China's IT success over twenty years today allows the Chinese Communist Party to impose its economic weight nearly worldwide to achieve both economic and political benefits as a rising global cyber power. While China's ability to preserve the economic gains and assure future freedom of international maneuver and influence rises, westernized states are still unable to make individual or like-minded collective economic defense strategies to ensure their societies survive well in a coming world of economic and political systems dominated by "Chinese characteristics."

Fourth, similar conceptual, narrative, and modeling struggles with integration into the whole-of-society national security for a deeply cybered world exist for westernized defense structures and participants. Several of the discussion's recommendations included new structures for the westernized democracies, finally shedding the legacy Cold War thinking to adapt to a cybered, hostile world. Especially critical are new institutional forms across defense, other public sector entities, and the private sector that operationally combine the magnitude of the IT talent, demographic weight, and inter-organizational joint operations experience of the 900 million-plus consolidated democratic civil societies. Militaries will be playing critical roles in the cybered conflicts of the future, but they will need to have constructed more flexible structures and strategies for allied, coordinated, and yet degraded, decomposable operations. National defense strategies will need to be aligned with national economic defense strategies. New forms of reserves, national

service, and integration with the private sector will need to be developed, gamed, implemented, and adaptively abandoned or evolved as major new basic IT investments produce advances to help defense overmatch particularly Chinese massive public support to its rising IT dominance. Military units should less and less mirror the standing massed forces of the Cold War, and yet be able to mass talent, persistence, and effects as needed for the whole-of-nation defense. Ultimately for militaries, cyberspace and cybered fleet or unified command analogies will have to be rethought to apply lessons learned from the history of minority states. For them, systemically combining operationally and across sectors was the only way to successfully resist aggressive larger states over the longer term; the challenge is the same in the cybered and hostile world.

This journal issue addresses these and other points in a variety of approaches. Together these pieces contribute to cyber security mid-level theory in offering the elements of broader systemic thinking to be used in research and, ultimately, in the development of new models and theories. To be clear, new model and theories are needed urgently for westernized democracies to adapt well enough to defend their economic well-being and room for maneuver for decades to come. The final objective is for these nations to buy time in the near term and adapt for the longer term, assuring they will be collectively thriving democratic civil societies in a hundred years despite being a minority of states in the larger emerging, adversarial, and cyber authoritarian world.

https://digitalcommons.usf.edu/mca/vol3/iss2/1
DOI: https://doi.org/10.5038/2378-0789.3.2.1053