Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 3 | Issue 1 Article 1

2018

Introduction to MCA Issue, "Cyber, Economics, and National Security"

Chris C. Demchak
chris.demchak@usnwc.edu

Introduction to MCA Issue, "Cyber, Economics, and National Security"

Chris C. Demchak, Issue Editor
Benjamin H. Schechter, Assistant Editor

Representing less than ten percent of the global population, consolidated democratic states have a steadily diminishing capacity to drive or deter what the remaining ninety percent of the world population does with cyberspace. This has implications for internet freedom, the rights of the individual, the uses of technology, and even the rules of the international economic system. The open question is not whether the civil societies can rule the future international system, but to what extent the largely authoritarian rest of the world rules the economic well-being and choices of these outnumbered democratic states. The range possible rests across three futures: from chaotic and disorganized isolated states looking much like today (Cyber Status Quo), individual state's sovereign cyber jurisdiction (Cyber Westphalia), or some form of a collective democratic like-minded response in the face of an authoritarian cyber hegemon (Cyber Resilience Alliance). Meanwhile, of the various academic fields economics stands out as the discipline least advanced in rethinking its industrial age models for a deeply digitized, conflictual, and upending new world order, especially its assumptions about free markets, rules of law and contracts, and the international liberal economic system.

The articles in this issue address challenges related to these different futures and the need to rethink economic assumptions, along with the role of cyber sovereignty, in democratic state efforts to avert the creeping loss of independent economic capacity and effective national defense in the rising post-western cybered world. The authors and the issues arise from two successive workshops held at the U.S. Naval War College late 2015 and 2016 addressing the futures and the economic models challenges. Two themes emerged, which these articles build off. One is the need to challenge economic assumptions to update the field's thinking about the emerging world and its financial realities that are so different from the post-WWII world in which those assumptions evolved into models. For a state, economic robustness is essential to being able to afford the talent, IT, and innovation necessary to defend in the increasingly more conflictual world. Similarly, a second theme is the role of a rising 'Cyber Westphalia or individual state's cyber jurisdiction in the challenges faced by states trying to modernize their national defense strategically, legally, and economically.

This issue is the first of series intended to widen and deepen the aperture of cyber defenders in understanding the wider global challenges beyond the cyber campaigns that occupy their daily lives. Cyberspace is now a 'substrate' underpinning the whole of society around us. However it was poorly coded, and hastily constructed, and now links all the social, economic, and technical systems we defend into a huge complex socio-technical-economic system (STES). For that reason, this wide-ranging and future-oriented issue is critical for military cyber defenders in particular. Of all folks in the field, cyber defenders need to have the widest view of the battlespace – the whole set of national STESs involved and its good and bad actors – to defend ourselves and our allies effectively. Times will be tough ahead. We need to prepare for the coming rise of a much larger cyber-competent world with an authoritarian anchor state that is not fond of democracy and not willing to leave us or our allies – and our national wealth – in charge of the world system.

Editors