Chapter 3
Thinking Systemically About Security and Resilience in an Era of Cybered Conflict

Peter Dombrowski
US Naval War College, USA

Chris C. Demchak
US Naval War College, USA

ABSTRACT

The international system now depends on cyberspace, a global 'substrate' of massive, complex, insecurely designed networks providing systemic advantages to masses of predators and adversaries. States today face an unprecedented spectrum of 'cybered conflict' between peace and war with growing existential implications. Their piecemeal searches for defensible jurisdictions are creating a rising Cyber Westphalian world crisscrossed with gateways, holes, national cyber forces, and often partial, uncoordinated, or vague strategies. Over time, the world will have robust, midlevel, and poor cyber powers, with the first tier coercing the others and dominating the rules of exchange. Democratic civil societies are not guaranteed to be robust. For acceptable future societal well-being in a deceptive and opaque cybered world, decision-makers need a systemic approach based on the logic of complex socio-technical-economic systems (STES) to create the systemic resilience and disruption capacities across shareable (across allies/sectors) secure architectures essential to becoming a robust cyber power, which is the focus of this chapter.

INTRODUCTION

Cyber war is not coming (Arquilla and Rondfeldt 1993), but 'cybered conflict' is. For decades we have been warned of the possibility of digital Pearl Harbors (Wilson 2008) where network attacks lead to cascading failures of critical military, public and private systems. Recently, there has been a backlash against the shrillest warnings about cyber war. Contrarians now argue that cyber war not only hasn't occurred but is highly unlikely (Rid 2012). They point to the absence of cyber "battle deaths" to date and the immense difficulty of using cyber weapons for political and military purposes. Botnets and malware

DOI: 10.4018/978-1-5225-7912-0.ch003

can disrupt service and lead to lost data but these are expensive nuisances rather than acts of war. Truly dangerous attacks, targeting, for example, the SCADA systems of military facilities or public utilities while potentially destructive, require exquisite intelligence and dedicated teams of hackers-- capacities beyond the means of most nation-states much less terrorists or common criminals.

Yet worrying about cyber war and arguing about whether it can occur or not misses something important about the contemporary security environment much less the future. Our communications networks and computer are vulnerable. Everyday new reports come of possible Russian attacks on Ukrainian websites; retail stores losing the personal data of customers to criminals, and next generation weapons allegedly developed using stolen engineering specifications. Adversaries of all sorts will seek to influence outcomes by accessing and altering both the systems themselves and the data that resides within. From hot shooting wars to spying by peacetime rivals much of the action now takes place within computer networks. The damage may be financial or reputational but the costs are real. For militaries, boots on the ground and ordinance on targets may be the ultimate determinants of victory, but to deploying soldiers in the field or launching missiles on now requires the secure, accurate, and timely flow of information.

The computer and telecommunications systems that comprise the backbone of modern militaries are both linked to, and part of, cyberspace. Even data encryption, the creation of closed systems and the establishment of air gaps between critical computer systems and outside networks have proved unreliable defensive measures against some advanced persistent threats (Singer and Friedman 2014: 55-60). As such hostile actors can disrupt and perhaps even destroy military systems in crises and wartime using techniques, tactics and procedures similar to those (but not limited to) used against private citizens, commercial firms and civilian government agencies.

If this isn't war, what is it? In this chapter we argue that the globe is enduring a period of cybered conflict in which states (including military organizations, intelligence agencies, and law enforcement), firms, and criminal are using cyberspace as a convenient medium for spying, attacking, and stealing from other entities reliant on computer and communications networks—that is virtually every social organization in the information age.

We conclude that, from the standpoint of nation-states (and social organizations in general), analyses of the security threats posed in and by "cyberspace" should adopt a systemic approach adapted from the logic of complex socio-technological systems (STES) (Trist 1980). Since such systems are "patterns of artifacts, institutions, rules and norms assembled and maintained to perform economic and social activities" (Berkhout, Smith, and Stirling 2003), scholars, policy-makers, and strategists needs to think through how emerging technologies from 3D printing to autonomous private vehicles to adoption of materials like grapheme will change those patterns (Manyika, Chui, et al 2013). Many arguments about how to respond to the security challenges posed by cyberspace taking place today in the government and policy communities are characterized by hype, false or misleading analogies (Betz and Stevens 2013; Goldman and John Arquilla 2014), and, worse, misunderstandings of the technical, engineering and scientific underpinning of critical terms and concepts. Instead, the conversations should be about how computer and communications are being penetrated and data is being lost, corrupted or stolen on a vast scale, and the harm done to victim societies as a whole. The focus of decision-makers must be to design and develop architectures—both technical and institutional—that can survive and prosper in the face of near constant attacks and evolving threats. To complicate matters, emergent technologies, sometimes labeled as disruptive technologies (Christensen 1997), may change the calculus, some reducing scale, proximity, and precision necessary for both bad actors and good to conduct offensive and defense cyber operations at any time (Pierce 2005; Dombrowski and Gholz 2006).