Chapter 12
Cyberspace as a Complex Adaptive System and the Policy and Operational Implications for Cyberwarfare

Albert Olagbemiro
United States Air Force Reserve, USA

ABSTRACT

The overall implication of depicting cyberspace as a complex, adaptive ecosystem rather than its current representation as a bi-dimensional domain provides an avenue for further insight into the complexities associated with operating in cyberspace. This renewed perspective brings to the forefront the critical role of the civilian private sector in cyber warfare, due to the intermixing and heavy reliance of the United States Government (USG) on an infrastructure owned and operated by the civilian private sector. The implications of such a revisionist perspective leads to a theory of action, which suggests that given this heavy reliance of U.S.G entities to include DoD, on a cyber-infrastructure predominantly owned and operated by civilian private sector entities, authorization to wage offensive-styled cyber-attacks, as a defensive measure should not be limited exclusively to the DoD but also expanded to include authorized entities in the civilian private sector.

INTRODUCTION

Actors across all levels of society use cyberspace with each actor having different roles, motivations, and intentions and the associated complexities of safeguarding cyberspace contribute to the lack of a United States Government (U.S.G.) policy for operating in cyberspace. This conceptual disorder stems from the current definition of cyberspace which fails to acknowledge the human dimension of cyberspace and the multiplicity of variables resulting in emergent properties, which arise due to the co-mingling of both public and private sector actors in cyberspace. The result is a form of social entropy in which social distinctions between state and non-state actors all but disappears, leading to a situation of jurisdictional

DOI: 10.4018/978-1-5225-7912-0.ch012

arbitrage in which both state and non-state actors are able to exploit the relative anonymity in which cyberspace confers during cyber operations (Kshetri, 2005, p. 541-62). To counter the status quo a paradigm shift is required, one that rejects the prevailing conventional science and embraces a revolutionary approach (Kuhn, 2012, p. 5-6). This transition from a conventional to a revolutionary science requires a new theory of the phenomenon of cyberspace which suggests that cyberspace is not a domain, but is rather a *socio-ecological ecosystem (SeE)*—an instance of a dynamic, complex, adaptive system that exists within a much larger information environment, known as the infosphere. This infosphere serves as the overall universe of physical and cognitive communication processes, and it is what constitutes the domain. By conceiving cyberspace as a SeE, the complexities associated with operating in cyberspace begin to emerge and provides insight into potential policy options for operating in cyberspace.

Given the current lack of a coherent U.S.G. policy, the objective of this paper is to illustrate how the tenets of complexity theory could provide additional insights and hopefully a roadmap for operating in cyberspace. These findings have significant operational implications for the Department of Defense (DoD) that could help shape the development of a coherent policy for operating in cyberspace. Achieving the stated objective first requires bringing coherence to current reasoning in the state-of-the-art. This is accomplished by developing a broad, ontological taxonomy of cyberspace. A new theory of the phenomenon of cyberspace is then proposed, from which an operational theory for operating in cyberspace is derived. Finally, the policy and operational implication of this new theory is discussed.

SEEDS OF COMPLEXITY

The term cyberspace is fundamentally an abstraction. As an abstraction, it manifests itself into physical reality through the Internet. Actors across all levels of society use cyberspace, each actor having different roles, motivations, and intentions. The physical manifestation of cyberspace is necessary because it needs an underlying means to exist in the physical realm—a mechanism, which the Internet provides in the form of a worldwide, publicly accessible series, of interconnected computer networks. The concept of open architecture networking was central to the design of the Internet with the idea of individual networks, independent of each other, possessing and presenting their own unique interface for integration, thereby creating a network of networks.

While the concept of open-architecture networking is the most powerful feature of the Internet, it is also its weakness. Since anyone can connect to the Internet without constraints on the types or geographic scope of networks, this makes it simple for hostile cyber participants to connect to the Internet. Furthermore, communication within this network of networks is primarily enabled by commercial entities through multiple interconnected backbones, called "Tier 1" providers, which provide the underlying infrastructure (e.g., routers, switches, etc.) through which data is transmitted. As of 2014, Tier 1 providers carry up to 98 percent of all U.S.G. communication traffic (Jensen, 2010).

Given the heavy reliance of the U.S.G. upon a physical infrastructure controlled and managed by non-state entities in the civilian private sector, this makes civilian infrastructure and civilian providers legitimate targets under the law of armed conflict. Further complicating the situation are the unintended consequences that can arise during a cyber-attack due to commingling of U.S.G. and civilian actors. The result is a form of social entropy in which social distinctions between state and non-state actors all but disappears, leading to a situation of jurisdictional arbitrage in which both state and non-state actors are able to exploit the relative anonymity in which cyberspace confers during cyber operations (Kshetri,