Establishing Cyber Warfare Doctrine

Andrew Colarik and Lech Janczewski

Introduction

Over the past several decades, advances in technology have transformed communications and the ability to acquire, disseminate, and utilize information in a range of environments. As a result, modern armies have advanced their command-and-control capabilities by using a robust information space through network-centric warfare. The ever-increasing convergence of military and commercial operations warrants considering the possibility that communication and information infrastructures are viable components – both as targets and weapons – in times of war.

Developments in recent years indicate that Internet and communication technology (ICT) in particular are becoming a viable theater of military conflict. The possibility of widespread conflicts fought in cyberspace continues to arise as digital-warfare capabilities are developed. The deployment window for a cyber attack has a dramatically different form from traditional conflicts and thus requires a different planning defense structure. Such an attack could be quickly prepared by a relatively small group, launched without warning from anywhere on the globe against any possible ICT target, and escalate in a matter of minutes to shut down national infrastructures (Parrish 2011). In this context, each modern state should be prepared to be the target of a cyber warfare attack and stand ready to launch a counteroffensive. Preparations for such conflicts have already started in many other countries, including Israel, North Korea, Iran, and Russia (The Economist 2010). When we examine these activities from a more holistic perspective, the preparation for both offensive and defensive cyber capabilities has both technical and public-policy components. In other
words, nations need to find answers and solutions to questions such as the following:

- What activities must be undertaken in the case of a cyber attack against a nuclear power plant?
- What is the measured and appropriate response to such an attack?
- What level of attack threshold constitutes an act of war?

With cyber attacks, there is no time to deliberate a comprehensive response. We believe modern nations lack a grand strategy for handling cyber attacks, one that gathers and coordinates their national resources for shared security and prosperity (Liddell-Hart 1967). Hence, we suggest that each country develop a cyber warfare doctrine (CWD) that includes all stakeholders, brings about a decisive conclusion when such attacks occur, and serves to deter future conflicts through a unified national security policy.

Developing a comprehensive CWD is a complex task requiring much preparation. Nevertheless, both civilian and military establishments have made considerable progress toward securing their national infrastructures and preparing for war in the cyber realm. Unfortunately, these efforts are being developed and implemented in a piecemeal manner. The planning components of both civilian and military interests are separate and disjointed, regardless of provisions that both sides believe will create synergistic outcomes (The White House 2011). What’s missing is a true systems approach to handling conflicts originating in cyberspace that cross many jurisdictional boundaries and interests. What’s needed is a general national policy on how to handle IT-based attacks that disturb a country’s normal functioning. Such a policy should embody a set of self-defense principles inclusive of civilian infrastructure, military objectives, and national security policy. This article argues for establishing a CWD that would be used to determine a nation’s appropriate response when attacked via cyberspace. Such a doctrine would be used as a guide for defense forces in a time of conflict; as a unified governing philosophy for military operations, deployment to protect civilian infrastructure, and the governance of international cyber relations; and as a deterrent to future adversaries.

The objective of this article is to summarize the considerations that would allow senior leadership to develop a comprehensive, strategic CWD. We will discuss the justification for considering information technologies in military conflicts and the events supporting our supposition, the various doctrines that will form the basis for developing a CWD, and the possible components of a CWD. We will also propose a national collaborative framework for obtaining stakeholder buy-in for a CWD and offer some final conclusions.