Journal of Strategic Security

Volume 5
Number 1 *Volume 5, No. 1: Spring 2012*

Article 7

Establishing Cyber Warfare Doctrine

Andrew M. Colarik Ph.D.
The University of Auckland

Lech Janczewski D.Eng
The University of Auckland

pp. 31-48

Recommended Citation
Colarik, Andrew M. Ph.D. and Janczewski, Lech D.Eng. "Establishing Cyber Warfare Doctrine." *Journal of Strategic Security* 5, no. 1 (2012) : 31-48.
DOI:
http://dx.doi.org/10.5038/1944-0472.5.1.3

Available at: https://scholarcommons.usf.edu/jss/vol5/iss1/7

Establishing Cyber Warfare Doctrine

Abstract

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. Modern societies and their respective militaries have taken advantage of a robust information space through network-centric systems. Because military and commercial operations have increasingly converged, communication and information infrastructures are now high-priority military objectives in times of war. This article examines the theoretical underpinning of current cyber warfare research, what we have learned so far about its application, and some of the emerging themes to be considered; it also postulates the development of a (national) cyber warfare doctrine (CWD). An endeavor of this scale requires lots of considerations and preparation for its development if it is to be cooperatively embraced. This article considers why information technology systems and their supporting infrastructures should be considered legitimate military targets in conflicts, and offers several events that support this supposition. In addition, it identifies the various forms of doctrine that will become the basis for developing a CWD, discusses a CWD's possible components, and proposes a national collaborative and discussion framework for obtaining a nation's stakeholder buy-in for such an endeavor.

Journal of Strategic Security
Volume 5 Issue 1 2012, pp. 31-48
DOI: 10.5038/1944-0472.5.1.3

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

Establishing Cyber Warfare Doctrine

Andrew Colarik and Lech Janczewski
Independent Consultant and University of Auckland

Abstract

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. Modern societies and their respective militaries have taken advantage of a robust information space through network-centric systems. Because military and commercial operations have increasingly converged, communication and information infrastructures are now high-priority military objectives in times of war. This article examines the theoretical underpinning of current cyber warfare research, what we have learned so far about its application, and some of the emerging themes to be considered; it also postulates the development of a (national) cyber warfare doctrine (CWD). An endeavor of this scale requires lots of considerations and preparation for its development if it is to be cooperatively embraced. This article considers why information technology systems and their supporting infrastructures should be considered legitimate military targets in conflicts, and offers several events that support this supposition. In addition, it identifies the various forms of doctrine that will become the basis for developing a CWD, discusses a CWD's possible components, and proposes a national collaborative and discussion framework for obtaining a nation's stakeholder buy-in for such an endeavor.

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.[1]

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.[2] 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:

- 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.[3] 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 infrastruc-

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

tures 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.[4] 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.

Setting the Stage: Milestones in Cyber War

In his celebrated book, *On War*, Carl von Clausewitz defines war as merely a duel on an extensive scale.[5] While such conflicts commonly occur between two parties, sometimes they enlarge to encompass multiple states, regional alliances, and federations of nations, in which the conflict is essentially between two sides; for example, the Axis Powers and the Allies in World War II. These types of wars, generally called symmetric, are often characterized by large conflicts between sides of relatively equal strength, resources, and technological capabilities. For many reasons—such as international treaties, global governance initiatives, and advances in military technology—these duels are becoming less frequent. Two of the biggest conflicts in recent years, in Iraq and Afghanistan, started as duels but quickly migrated toward a different type of conflict: asymmetric war.

In its simplest form, "have-nots" undertake such warfare against "haves," seeking victory by employing their specific advantages against the vulnerabilities of a much stronger opponent.[6] To overcome the disparity in strength, the weaker antagonist looks for asymmetric options, targeting the "will" of the stronger opponent by strategically pursuing disproportionate psychological effects.[7] In the authors' view, being able to turn opponents' greatest strengths into their greatest weaknesses is the highest, most refined form of asymmetric warfare.

For decades, adversaries have compromised the use of information technology by stealing financial, proprietary, and/or secret information, and continue to do so today.[8, 9] So dependent on technology have modern nations become that they are fundamentally weakened when such systems and processes are disrupted for any meaningful time. This vulnerability, of course, continues to have national security implications. As a result, numerous national and international efforts have been made to develop policies for combating the use of cyberspace for criminal activities.[10, 11, 12, 13, 14]

In recent years, a series of milestones have provided clear indicators for the viability of asymmetric conflicts originating in cyberspace. The most significant of these have involved the European nation state of Estonia, which has implemented a highly integrated e-government infrastructure. The country was forced to digitally isolate itself when unknown, politically motivated attackers initiated a series of distributed denial of service (DDoS) assault incorporating one-million-strong botnet. The attacks on Estonia's Internet systems began in April 2007 and lasted three weeks, but it is their sustained impact that's of primary importance to this discussion, rather than the technological methods employed.[15] We believe the attacks, which the Estonian government has labeled "cyber terrorism," have provided the impetus for nation-states to deploy cyber-offensive capabilities for future conflicts.

Another milestone were the cyber attacks on the former Soviet-bloc state of Georgia, which mimicked the events that occurred in Estonia. The country's national communication infrastructure was shut down just before Russian military forces entered its borders in August 2008. Government websites and news outlets as well as banks, including Georgia's largest, were affected. While the country's use of the Internet is still emerging, the effects of the attacks limited the government's ability to spread its messages in time of crisis. Efforts to engage and perpetuate the cyber attacks during this period were consistently conducted in Russian, but no verifiably responsible party has been identified to date.[16]

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

The last milestone relates to the first detection of a new breed of computer worm known as Stuxnet, which appeared in June 2010. It is considered the first worm specifically created to target real-world infrastructure, such as power stations and water plants. After it has hijacked a PC, Stuxnet looks for Siemens software that runs industrial control systems and begins to speed up or slow down power generation for destructive means, which was the case for Iran's Bushehr nuclear plant. The worm's resemblance to legitimate software, such as digital certificates, while using a self-launching, zero-day vulnerability in the attack, allowed its rapid, unobstructed distribution through the *a priori* assumption of security software that if a program meets certain conditions, it is trustworthy.[17]

The ramifications of the above milestones to national infrastructures in times of conflict are staggering. Not only can a nation's communication channels be disrupted as a force multiplier, but basic infrastructure, such as power and water distribution, can also be remotely attacked and disabled, putting the targeted country at a distinct disadvantage. The military establishments of many countries have for some time recognized the possibility of a cyber war, and we believe the above milestones were the impetus for both the viability and necessity of recent cyber mobilizations. A 1996 report prepared for the U.S. Office of the Secretary of Defense projected that battlefield Command, Control, Communications & Intelligence (C3I) vulnerabilities "may become less significant than vulnerabilities in the national infrastructure."[18] In June 2009, the U.S. Cyber Command was created, and in July of 2011, Deputy Secretary of Defense William J. Lynn III announced that as a matter of doctrine, cyberspace will be treated as an operational domain similar to land, air, sea, and space.[19, 20] In their notable book, *Unrestricted Warfare*, Chinese colonels Liang and Xiangsui claimed advanced technology gave the country's adversaries a significant advantage, and proposed that China "build the weapons to fit the fight."[21] Recently, the Chinese People's Liberation Army (PLA) confirmed the existence of its Online Blue Army.[22] Many smaller countries have also begun developing cyber warfare divisions, but thus far have kept such capabilities plausibly deniable or at a low profile to avoid preemptive reprisals.[23]

All of the above are major indicators that information technologies are already playing an important role in carrying out military objectives. These examples are but a small collection of high-profile cases, and we believe sufficient evidence points toward countless lower-profile events that have gone unreported or been classified. In the next sections, we will discuss the theoretical foundations of national doctrine in preparation for addressing the larger strategic importance of technology's role in achieving military objectives.

Doctrine

In its simplest form, a doctrine is defined as a body of principles that form a system of belief. A doctrine can be considered a statement of fundamental government policy; a principle of law established through past decisions; or a military principle or set of strategies.[24] In essence, a doctrine embodies the rules by which individual societies govern themselves and maintain standards. Therefore, a CWD in principle represents a set of rules and standards for governing a war involving cyberspace. When viewed in more depth, a doctrine brings with it a set of characteristics stemming from the people who embrace it and their societal processes. Doctrine functions to: provide a tempered analysis of experience and a determination of beliefs; teach those beliefs to succeeding generations; and offer a common basis of knowledge and understanding that can provide guidance for action.[25] In other words, doctrine states how to do something the best possible way, and is passed on to subsequent generations. This implies that it is based on knowledge accumulated from making strategic decisions within a domain. Therefore, doctrine may take many forms, either fact-dependent and limited in scope, or broadly interpreted and sweeping in its breadth of application.[26]

To form a CWD, the dominant doctrines governing a people's lives must be examined. The authors believe a CWD must reflect the accepted doctrines governing how we organize and direct ourselves, interact with others, pursue prosperity, and defend ourselves collectively if future generations are to sustain and support it. In the following section we shall briefly examine three dominant doctrines. The first is political, which is most often reflected in a nation's constitution or its equivalent. The second is legal, which often follows political doctrine as an embodiment of societal interaction. The last is military, which governs how a nation secures itself.

Political Doctrine

Throughout much of the West, it is traditionally understood that open, democratic societies must have a set of common understandings or governing principles that allow people to mutually interact. These principles are articulated through political doctrine, which establishes the political and social structure of a nation and the supporting structures that grow from its principles and shape the doctrine's impact on future generations. An example of political doctrine is a constitution, which may be considered a set of fundamental principles, or established precedents, according to which a state or other organization is governed.[27]

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

We believe the political doctrine embodied in a nation's constitution articulates the will of a people, a new order, a new way of governance, or a new social doctrine. It is in this document that the prevailing political principles for governing reside, and are used to shape a society's social and legal environments. A national constitution is usually a mirror of a nation's past and a prescribed program for its future. An example of such a document is the U.S. Constitution, adopted in 1787 at a critical moment in the country's history. Major conflicts with Spain and England remained unresolved; large amounts of capital had been drained by the war of independence; and a substantial number of states were unsure about union membership. The country needed an efficient system of national government while maintaining individual states' rights. The Constitution's preamble reflects this by stating: "We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defence, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America." The document was created at a pivotal point in history, when American society was compelled to choose the manner in which it would govern itself. We believe that to be consistent with a society's values and internal processes, a CWD must embrace its principles, as illuminated in a document such as a constitution.

Legal Doctrine

Once it embraces a political doctrine, a nation must invoke systems and processes that exemplify its "spirit." These are often articulated in its legal doctrine, considered the currency of the law, in that established precedent becomes the foundation for determining the application of law in future cases. In law, rules tend to be strict requirements that identify the answer to a dispute once the facts have been established, while standards are more like guides for resolving disputes after identifying a set of factors to be considered and balanced.

One of the dominant doctrines in law is *Stare Decisis*, Latin for "Let the decision stand." This is a legal principle by which judges are obliged to respect the precedents established by prior decisions. This overarching principle guides courts in following standards established by decisions in earlier cases.[28] Thus, judicial activism is minimized and consistency in future judicial rulings is established, allowing a people to better understand their current and future legal obligations when interacting with one another. With *Stare Decisis* in mind, we strongly suggest that any new doctrine, including a CWD, must be based on a country's current legal doctrine and established precedents. There may be times, when new pre-

cedents must be established—for example, when technological developments impact politics and the economy—but while they may help a nation better handle recurring problems, they may also create unforeseen consequences and dysfunctions between the law and its enforceability. The authors therefore caution the framers of a CWD against forcing new precedents without fully considering their possible consequences.

Military Doctrine

Once a nation has decided on its basic political and legal doctrines, it must address how it intends to defend itself and its chosen way of life. Military doctrine embodies the fundamental principles by which a country's military force guides its actions in support of national objectives.[29] This doctrine can in turn be divided into fundamental, environmental, and organizational doctrines, which identify key military factors and address how each will be governed and under what conditions. The nature of war, as well as the purpose of military forces and their relationship to other instruments of power, reside in fundamental doctrine, which is relatively insensitive to political philosophy or technological changes. The following examples are typical statements of fundamental doctrine:

- War is the failure of policy.
- The object of war is to overcome an enemy's hostile will.
- The object of war is a better state of peace.

The fundamental portion of a CWD may include such statements as governing principles in developing environmental and organizational components. The cumulative understanding of military deployment in a particular operating medium—such as sea, air, land, and space—forms environmental doctrine. In the case of a CWD, the environment is likely to embody information technologies and computer networks, and their physical infrastructures. Organizational aspects likely will be adaptations of existing structures. Both environmental and organizational components will require consideration throughout the CWD development process.

Developing CWD Components

Considering the many details critical to formulating a CWD, serious consideration of a collaborative and discussion framework is crucial. This section offers a conceptual starting point and present several key strategic questions we believe essential to forming a cyber warfare doctrine. We

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

offer these questions as critical examples of the types of queries needed to enable a corrective and decisive response following an attack. (These types of queries will form the foundation of the last section of this article.) Our proposed questions are:

What is the line between cyber warfare and traditional warfare?

Definitions matter when implementing policy, and in developing a CWD a variety of factors must be considered. In essence, this question focuses on the role of information technology as an enabler of warfare and, therefore, as a viable target from both attack and defense viewpoints. We believe cyber warfare will have kinetic world effects, meaning it will cause real direct and indirect damage to physical infrastructure.[30] The notion that an information-age war would be bloodless and sterile is challenged by the fact that our digital infrastructures and physical capabilities are integrated in order to sustain and support modern warfare.[31]

Information is the central element for commanding the conflict space; of equal importance is the infrastructure that allows information to flow. From a strategic perspective, we must consider an opponent in a cyber war as a system composed of a series of subsystems.[32] Each subsystem that supports and sustains the larger system enables a country to direct its resources toward the conflict. The essential question before us is: To what extent will a cyber warfare conflict encompass real-world assets and lead to full-scale war? Without a clear distinction between cyber and traditional warfare, how can any country in the modern world take action that is justified, rational, and proportional to a given attack? We believe such a distinction is crucial.

What is the CWD conflict space?

Controlling the conflict space is central to resolving military conflicts. But when a country seeks to do so, what exactly are its objectives? The authors believe cyber warfare involves preventing opponents from knowing as little about you while you seek to know everything about them.[33] This "knowledge battle" extends to a nation controlling its own resources while rendering its opponent's ineffective.

Preventing the use of resources is central to controlling the conflict space. In an increasingly interdependent global economy, the implications can quickly escalate to encompass unforeseen consequences. Battle space dominance likely will include a nation's information infrastructure as well as the information flowing through it from both sides of the conflict. We

must also consider all of the pathways and infrastructure between the two parties in a conflict, as information infrastructures are rarely symmetric. These third-party pathways likely would be active or unwitting participants in attack and defense measures, as their infrastructures would support such activities. Because of the distributive architecture of cyberspace, defining the conflict space both in totality and in conflicts as they arise is the first step in developing strategies to control it.

What threshold of aggression constitutes the level of CWD response?

Waging a moral war is essential to sustaining it, and we believe a cyber war is no different. A measured response to a cyber warfare attack requires deterrence and escalation levels.[34] The strategic objective in a conflict is to cause an opponent's systems to change to such an extent that it is forced to adopt your objectives or become incapable of mounting an opposition. In a retaliatory action aimed at deterring future attacks, a CWD should establish responses that would cost the aggressor more than it might stand to benefit from such attacks, thereby encouraging restraint. If a significant penalty beyond an incident is not established, escalating attacks likely will occur. But to remain moral, such responses must be proportional. Thus, an assessment of any attack should be accompanied by a suitable and corresponding response to maintain its moral justification when damages or casualties are incurred. Therefore, determining the range of responses, along with their alignment with a nation's strategic security goals, is critical to responding responsibly to attacks.

What is the definition of a CWD victory?

War must be waged with a constant regard for the peace desired. As with a response and escalation policy, knowing what constitutes a CWD victory is essential to not overreaching. Responses to aggression must consider taking possession of the opponent's strengths as well as destroying its armed power, all while considering public opinion. Levels of desired outcomes must be tied to any attack response. Depending on the assault's severity, victory may be limited to restoring operations and taking steps to improve defensive measures. The prevention of future attacks would then be a consideration in establishing victory conditions. In larger-scale conflicts, the partial or complete disabling of an aggressor's attack capabilities may be warranted and considered a victory condition. When an aggressor has the full support of the country, the elimination of the attack infrastructure may be warranted, thus also serving as a victory condition.

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

The authors believe that a clear understanding of victory is crucial to the formation of a CWD, as it has profound policy implications for future peaceful relations with both the antagonist and the rest of the world.

What are the principal CWD assets needed to win?

A comprehensive understanding of the assets needed to wage a cyber war is essential to creating the infrastructure for supporting a CWD. Identifying the dependencies a military force has on information technology is tightly coupled with defining the needed assets. Modern militaries rely heavily on systems that provide speed of command in order to achieve information superiority and the massing of effects. The result of the rapid foreclosure of enemy action and the shock of closely coupled events makes network-centric operations a significant strategic advantage.[35] Assets that enable increased information richness, reach, and shared awareness are responsible for the transformation of improved awareness into collaborative planning and synchronized action.[36] Assets that provide for peacekeeping measures such as border management and verification activities play a role in threat awareness and removal.[37] We believe these assets, and any suitable measures to defend or attack them, must be identified to prevent a CWD from lacking the proper scope and depth when implemented.

What are the factors inhibiting an effective and decisive CWD response?

We live in a global community of communities, and the more integrated and interdependent the world becomes, the more our policies and responses will be moderated by those indirectly connected to our actions. Cyberspace is made up of core national and international infrastructures residing in a multitude of legal jurisdictions and global alliances. We believe that without fully considering the regional and global consequences of taking direct action in a cyber war, no CWD would bear a substantive relation to a nation's larger strategic security policy. By understanding this sphere of influence and articulating the implications, profound long-term ramifications can be mitigated and a greater understanding of state actors can be cultivated. The authors believe that a CWD should contain remedies for factors that would inhibit effective and decisive responses in any cyber war conflict. While additional issues undoubtedly will be raised while forming a CWD, we think the queries presented here are representative enough, in both depth and scope, to illustrate key elements that must be considered in such an endeavor.

Collaborative and Discussion Framework

The foundation of a nation's information infrastructure is generally distributive in nature, and the creation of a CWD is no simple task if it is to include its closest stakeholders. Drawing upon the past for guidance, the authors propose a collaborative and discussion framework similar to the one used by President Dwight Eisenhower in confronting the expansion of communism and the threat of nuclear war. The president believed the best way to formulate national policy in a democracy was to assemble the best-qualified people with opposing views on an issue and listen carefully as they debated it.[38] This approach formed the foundation of Project Solarium, which resulted in a doctrine that governed the Cold War, and whose effects are still felt today.[39]

We believe several fundamentals must be observed for a collaborative and discussion framework to be successful. The first of these is that a CWD initiative should be originated and governed by top government officials, as executive government is in the best position to facilitate and coordinate such an endeavor. Second, participating experts should be delegates from civilian government, defense, security, and professional organizations related to information technology, so that a broad set of skilled stakeholders are represented in the problem-formulation and solving processes. Third, a relatively short time should be allocated to creating a CWD, forcing participants to stay focused on the tasks at hand and not expand the mandate's range and scope. Fourth, the results of such an endeavor should be accepted by the nation's head of state and be widely published. This last step is critical, for the CWD's dissemination establishes new norms of conduct, and consequences for their breech. This doctrine transparency is in keeping with the highest traditions of open, democratic societies and clearly changes the rules of digital importance as a national security imperative.

The proposed framework has three phases. In Phase One, the head of a nation initiates the CWD collaboration process by identifying and selecting the primary stakeholders—from business, government, and professional organizations—who have both a vested interest in any CWD outcomes and the expertise to contribute substantively to the endeavor. Each organization selects delegates to represent it at a convention charged with creating a key set of questions such as those contained in the previous section.

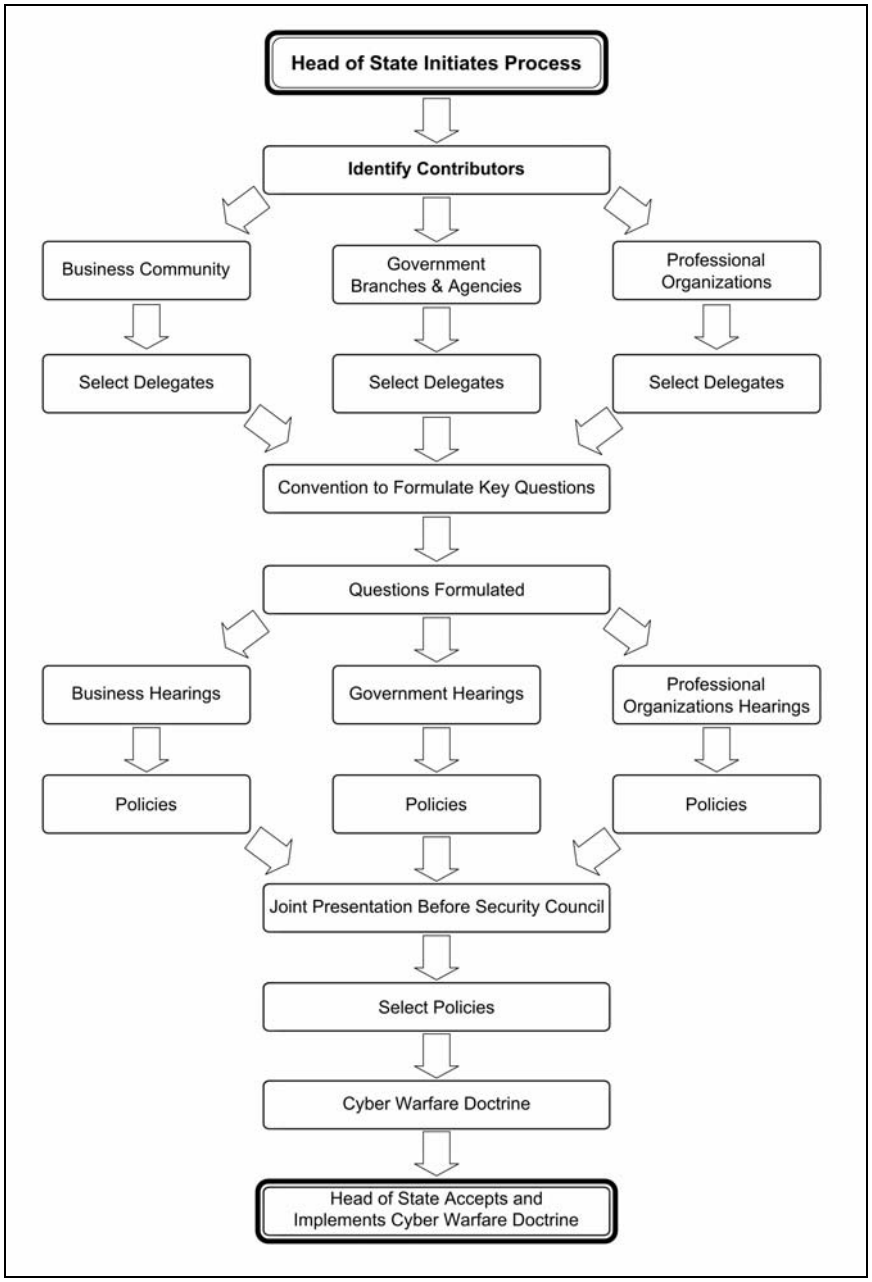
Once these questions have been agreed on, Phase Two commences, with the questions being sent to the selected organizations in Phase One for deliberation. Because knowledge is often held by unlikely participants,

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

and due to the larger implications of a CWD, the authors strongly suggest that these hearings be held in public forums, at which constituents may freely offer policy ideas in answering the key questions.

Once assembled by participating organizations, these policy suggestions form the basis of Phase Three, in which the business community, government branches and agencies, and professional organizations jointly assemble before the nation's head of state and security council to present their ideas for answering the questions, and to defend their proposals against opposing viewpoints. Critical to this phase is that all participants rigorously review the areas of discourse. It falls to the security council to assemble policies common among stakeholders, as well as those that have withstood rigorous examination by all participants. A final document is then formulated and presented for ratification.

The authors believe the above process would create a CWD that has stakeholder input and buy-in, that addresses a nation's main cyber war concerns, and that permits decisive action with the backing of the nation-state (see Figure 1).



https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

In summary, the proposed framework for developing a national CWD is based on several fundamental principles. The first is that such a venture would be conducted at the head of state's discretion, regarding both initiating the CWD process as well as its final acceptance. The CWD's development would be delegated to specialists from civilian government, defense personnel, security, and professional organizations related to information technology. The final proposals would be presented to the national-level security council (or other body with similar responsibilities) and ultimately be accepted by the head of state. The final CWD formulation would then be placed in the public domain.

Conclusions

Information technology has reached a level of development and integration into modern societies that allows it to be used to damage a nation's well-being. Numerous examples are available, and this article has presented several of them. Attacks on information systems and infrastructures may soon escalate into a full-scale military conflict. Whether such a confrontation is provoked by third-party cyber criminals or state-sponsored forces, a country would do well to be prepared. Many other defense forces are also developing or mobilizing themselves for cyber conflicts on a national and international level. To our knowledge, no state to date has a comprehensive national strategy for handling a cyberwar that aligns the civilian infrastructure with military operations in a collaborative environment. In this article, we have summarized many of the dominant issues that must be addressed to formulate a comprehensive national CWD. We have outlined a collaborative process that brings together the government, business, and professional organizations responsible for a country's cyber infrastructure and national security.

About the Authors

Dr. Andrew M. Colarik is an independent consultant, author, researcher, and inventor of information security technologies. He has published multiple security books and publications in the areas of cyber terrorism, information warfare, and cyber security. He has made presentations before a host of groups and organizations; has appeared on syndicated TV and radio shows such as Fox News, The 700 Club, and Coast to Coast; and is a Fox News contributing cyber security and terrorism expert. Dr. Colarik's research interests involve technology's impact on social, political, legal, and economic structures in society; the design and implementation of secure communication systems; and the evolving applications and

consequences of the global information infrastructure on businesses, governments, and individuals. For more information on Dr. Colarik, visit his website at: *http://www.AndrewColarik.com*.

Dr. Lech Janczewski has over thirty-five years' experience in information technology. He was managing director of the largest IBM installation in Poland, and project manager of the first computing center in Nigeria. He is an associate professor at the University of Auckland, Department of Information Science and Operations Management. His area of research includes data security management with a special emphasis on cyber terrorism. Dr. Janczewski has written about 300 articles presented in scientific journals, conference proceedings, and books. He is chairperson of the New Zealand Information Security Forum, secretary of the IFIP TC-11 committee (Security and Privacy Protection in Information Processing Systems) and Fellow of the New Zealand Computer Society. For more information on Dr. Janczewski, visit his website at: *http://staff.business.auckland.ac.nz/5283.aspx*.

References

1 K. Parrish, "Cyber Threat Grows More Destructive," *American Forces Press Service*, July 15, 2011.

2 "The threat from the internet, Cyberwar, it is time for countries to start talking about arms control on the internet," *The Economist*, July 1, 2010, available at *http://www.economist.com*.

3 Liddell-Hart, Basil Henry, *Strategy: The Indirect Approach*, 2nd revised ed. (London: Faber and Faber Limited, 1967), 430.

4 "International Strategy for Cyberspace," Washington, DC, U.S. White House (2011), available at: *http://tinyurl.com/3aovtx5 (www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)*.

5 Clausewitz, C., *On War* (London: N. Trübner, 1873), translated and edited by Hans W. Gatzke (The Military Service Publishing Company, 1952).

6 Thornton, R., *Asymmetric warfare: Threat and response in the twenty-first century* (Cambridge: UK Polity Press, 2007).

7 K. McKenzie, "The Rise of Asymmetric Threats: Priorities for Defense Planning," *Quadrennial Defense Review*, Chapter 3 (2001): 75–105.

8 Stoll, C., *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (NY: Pocket Books, 1989).

9 D. Alperovitch, *Revealed: Operation Shady RAT*, McAfee White paper, Publication No 33000wp_shady-rat_0811, August 2011, available at: *http://tinyurl.com/3jo20b2 (www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf)*.

https://scholarcommons.usf.edu/jss/vol5/iss1/7
DOI: http://dx.doi.org/10.5038/1944-0472.5.1.3

10 *Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo* (Washington, DC: Center for Strategic and International Studies, 1998).

11 "Convention on Cybercrime," Budapest, Council of Europe, 2001, available at: *http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm*.

12 "The National Strategy to Secure Cyberspace," Washington, DC, U.S. White House (2003), available at: *http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf*.

13 "Regulation (EC) No 460/2004: Establishing the European Network and Information Security Agency," European Parliament (2004), available at: *http://tinyurl.com/7qhlyc8 (eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML)*.

14 D. Eijndhoven, "Dutch Government to Design Cyber Defense Doctrine," INFOSEC Island, February 27, 2011.

15 K. Ruus, "Cyber War I: Estonia Attacked from Russia," *European Affairs* 9:1 (2008).

16 "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence, November 2008.

17 Matrosov, et al., "Stuxnet Under the Microscope," ESET Software, Revision 1.31, January 2011, available at: *http://www.eset.com/us/documentation/white-papers*.

18 R. Molander, A. Riddle, and P. Wilson, *Strategic Information Warfare, A New Face of War*, National Defense Research Institute RAND (1996).

19 "Cyber Command Fact Sheet," U.S. Department of Defense (October 13, 2010), available at: *http://tinyurl.com/7exploy (www.defense.gov/home/features/2010/0410_cybersec/docs/CYBERCOM Fact Sheet to replace online version on OCT 13.pdf)*.

20 W. Lynn, "Remarks on the Department of Defense Cyber Strategy. As Delivered by Deputy Secretary of Defense William J. Lynn, III," National Defense University, Washington, D.C., Thursday, July 14 2011, available at: *http://www.defense.gov/speeches/speech.aspx?speechid=1593*.

21 Liang, Q. and W. Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).

22 M. Lebowitz, "China military admits cyberwarfare unit exists," *Security News Daily*, May 26, 2011, available at: *http://tinyurl.com/6v2bssz (www.msnbc.msn.com/id/43189050/ns/technology_and_science-security/t/china-military-admits-cyberwarfare-unit-exists)*.

23 K. Fogarty, "North Korea steps forward as new cyberwar villain: March DDOS against South Korea may have been dry run for real attack," *IT World*, July 6, 2011, available at: *http://tinyurl.com/6h5a60d (www.itworld.com/security/180435/north-korea-steps-forward-new-cyberwar-villian)*.

24 *Webster's New World Dictionary and Thesaurus*, Second Edition (Wiley and Sons, 2002).

25 D. Drew and D. Snow, "Making Strategy: An Introduction to National Security Processes and Problems," Air University Press, Chapter 11, August 1988, 163–174.

26 E. Tiller and F. Cross, "What is legal doctrine?," *Northwestern University Law Review* 100:1 (2006).

27 *The New Oxford American Dictionary*, Second Edition (Oxford University Press, 2005).

28 R. Kozel, "Stare Decisis as Judicial Doctrine," *Washington and Lee Law Review* 67:2 (2010): 411.

29 *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, Joint Publication 1–02, November 8, 2010, 579.

30 R. Parks and D. Duggan, "Principles of Cyber-warfare," United States Military Academy, Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, West Point, NY, June 5–6, 2001, 122–125.

31 G. Sullivan and J. Dubik, *War in the Information Age*, Carlisle Barracks, PA, U.S. Army War College (1994).

32 J. Warden, "The Enemy as a System," *Airpower Journal* (Spring 1995).

33 J. Arquilla and D. Ronfeldt, "The Advent of Netwar: Analytic Background," *Studies in Conflict & Terrorism* 22:3 (1999): 193–206.

34 W. Tirenin and D. Faatz, "A Concept for Strategic Cyber Defense," IEEE Military Communications Conference, Atlantic City, NJ (1999).

35 A. Cebrowski, "Network Centric Warfare: Its Origin and Future," Naval Institute Proceedings (1998): 28–35.

36 Alberts et al, *Understanding Information Age Warfare*, Washington, DC, CCRP Publication Series (2001): 312.

37 T. Cahill, K. Rozinov, and C. Mule, *Cyber Warfare Peacekeeping*, West Point, NY, United States Military Academy, Proceedings of the 2003 IEEE Workshop on Information Assurance (June 2003): 100–106.

38 "Project Solarium," Eisenhower Memorial Commission, 2011, available at: *http://www.eisenhowermemorial.org/stories/Project-Solarium.htm*.

39 Eisenhower, D., *Minutes of 155th Meeting of NSC*, Papers as President, 1953–1961, NSC Series, Box 4 (1953).