Developing a Grand Strategy for Cyber War

Andrew M. Colarik
Department of ISOM
The University of Auckland
Auckland, New Zealand
a.colarik@auckland.ac.nz

Lech J. Janczewski
Department of ISOM
The University of Auckland
Auckland, New Zealand
lech@auckland.ac.nzm

Abstract— **This paper considers why information technologies should be considered in military conflicts and offers several events that support this supposition; identifies the various forms of doctrine that will become the basis for developing a Cyber War Doctrine (CWD); tenders a discussion of the possible components of a CWD; and a proposal for a national collaborative framework for obtaining stakeholder buy-in of a nation for such an endeavor.**

Keywords-component; Conflict, Cyber, Doctrine, Infrastructure, Military, National, Policy, Protection, Security, Strategy, War.

1. 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. Modern armies as a result have advanced their command and control capabilities utilizing a robust information space through network-centric warfare. The ever increasing convergence of military and commercial operations warrants the consideration that communication and information infrastructures are viable military objectives in times of war. Developments in recent years indicate that Internet and Communication Technology (ICT) in particular are becoming a viable theatre of military conflict. The possibility of wide spread conflicts fought in cyber space continue to rise as digital warfare capabilities are developed. The deployment window for a cyber attack has a dramatically different form than traditional conflicts, and as such requires a different planning defense structure. Such an attack could be quickly prepared by a relatively small group; launched without any warning from any place on the globe against any possible ICT target; and escalate in a matter of minutes to shut down national infrastructures [1]. This means that each modern state should be prepared for being the target of a cyber war attack and be ready to launch an effective counteroffensive.

The preparations for such conflicts have already started in many other countries such as Israel, North Korea, Iran, and Russia [2]. When we examine these activities in a more holistic perspective, the preparation for both offensive and defensive cyber capabilities have both a technical character as well as a public policy component in responding to such attacks. In other words, nations need to find answers and solutions to questions such as what activities need to 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; and what level of attack threshold constitutes an act of war. With such attacks, there is no time to deliberate a comprehensive response.

For decades, our use of information technology has been compromised by adversaries through the theft of financial, proprietary and/or secret information [3], and these continue to be exploited today [4]. The growing dependence on technology has also created a fundamental weakness when such systems and processes are disrupted for any meaningful time, and as such continue to have national security implications [5]. As a result, there have been numerous national and international efforts to develop policies for combating the use of cyberspace for criminal activities [6], [7], [8], [9], [10]. The problem with these efforts is that that are not inclusive of all stakeholder interests regardless of claims. It is in the opinion of the authors of this paper that modern nations today are lacking a grand strategy for handing cyber attacks that coordinates all of its resources towards defending the state for its mutual security and prosperity [11]. Hence, we offer that each country should develop a Cyber War Doctrine (CWD) that is inclusive of all stakeholders, brings about a decisive conclusion when such attacks occur, and serves to deter future conflicts through a unified national security policy.

In the following sections we will discuss: the identification of the various forms of doctrine that will become the basis for developing a CWD (Section 2); a discussion of the possible components of a CWD (Section 3); a proposal for a national collaborative framework for obtaining stakeholder buy-in for a CWD (Section 4); and our final conclusions (Section 5).

2. A SYSTEM OF SHARED UNDERSTANDING

For any unified national effort, people must be able to embrace and/or support a common set of understandings and these are often embodied through some form of doctrine. In its simplest form, a doctrine is defined as a body of principles that form a system of belief. It can be considered a statement of fundamental government policy; a principle of law established through past decisions; and a military principle or set of strategies [12]. In essence, a doctrine

embodies the rules and standards by which individual societies govern themselves and maintain those standards. Therefore, a CWD in principle represents a set of rules and standards for governing a war involving cyberspace. When looked at in more depth a doctrine brings with it a set of characteristics that stem from the people and their societal processes who embrace it. Doctrine functions to provide a tempered analysis of experience and a determination of beliefs; to teach those beliefs to each succeeding generation; and to endow a common basis of knowledge and understanding that can provide guidance for action [13]. Therefore, doctrine is what we believe about doing something in the best possible way and passing this knowledge on to subsequent generations. This implies that doctrine is drawn from accumulative knowledge in making strategic decisions about a domain. Therefore, doctrine may take many forms that may be fact-dependent and limited in scope, or broadly interpreted and sweeping in the breadth of its application [14].

The existence of some of the dominant doctrines that govern people's lives must be examined as these will better articulate the depth of doctrine as well as impact the formation of a CWD. In the authors' opinion, the accepted and prevailing doctrines that govern the aspects of how we self-organize and direct, interact with ourselves and others, pursue prosperity and defend ourselves collectively must be reflected in any CWD if it is to be sustained and supported in the long-term for future generations. There are three dominant doctrine themes we shall briefly examine in this section. The first of these is political doctrine, and this in the modern world is most often reflected in a nation's constitution or its equivalent. The second of these is legal doctrine, and this often follows political doctrine as an embodiment of societal interaction. The last is military doctrine which governs how a nation seeks to secure itself.

As a means to demonstrate political doctrine, we offer that a constitution can be considered to be a set of fundamental principles or established precedents according to which a state or other organization is governed [15]. It is the authors' view that the political doctrine outlined in a nation's constitution is a means for articulating the will of a people, a new order, a new way of governing a county, and/or establishing a new social doctrine. It is in these documents that the key expressions of prevailing political principles for governing reside and are used to shape the social and legal environments of a given society. A national constitution is usually a mirror of a nation's past and a prescribed program for its tomorrow. Let's look on some these documents.

The current French constitution was accepted in 1958, but the foundations of law for France were set up during the French Revolution between 1789 and 1799. The revolutionaries' aim was to overthrow the monarchy and introduce democratic principles to the land. The monarchy was despised by a majority of its society for its corruption, selfishness and lack of moral standards. The revolutionaries wanted to create a country that provided equal rights to everybody, followed the law, and to build a more cohesive society. Hence their slogan: Liberté, égalité, fraternité (Liberty, Equality, Fraternity). To reflect these principles, article 2 of the French constitution states "The principle of the Republic shall be: government of the people, by the people and for the people".

The U.S. constitution, adopted in 1787, was introduced in a critical moment of that country's history. The U.S. had major unresolved conflicts with Spain and England, the war of independence had drained large amounts of its capital, and a substantial number of states were not sure if they wanted to be a part of the union. As such, there was a need to create an efficient national system of government while maintaining individual state rights. It is reflected in the preamble of the US constitution which states "We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defense, 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 above are examples of two pivotal points in history when a society had to choose the manner in which they will be governed. The above briefly illustrates the importance of political doctrine in setting the political and social structure of a nation, the structures that grow from such prevailing principles and its impact on future generations. We believe that a CWD must embrace a nation's intended principles outlined in such documents in order to be consistent with a given society's values and internal processes.

Once a political doctrine has been embraced, a nation must invoke systems and processes that exemplify its spirit and these are often articulated in its legal doctrine. Legal doctrine is considered the currency of the law in that established precedent becomes the foundation to determine 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 guides for resolving disputes after identifying a set of factors to be considered and balanced [14]. One of the dominant doctrines in law today is *Stare Decisis* which means "Let the decision stand" in Latin, and is a legal principle by which judges are obliged to respect the precedents established by prior decisions. It is this overarching principle that guides courts to abide by standards that have been established by decisions in earlier cases [16]. In this way, judicial activism is minimized and a consistency in future judicial ruling allows a people to better understand their current and future legal obligations when they interact with others. From *Stare Decisis*, we may strongly suggest that any new doctrine, including a CWD, should be based on the current legal doctrine of a country and the precedents that it has established. In most cases, this principle works. However, with the developments of technology and its impact on politics and economy, there may be times when new precedents must be established. These new rules could better help a nation handle their re-occurring problems. They may also create unforeseen consequences and dysfunctions between the law and its enforceability. The authors caution any framers of a CWD in forcing new precedents without considering the consequences of it in a myriad of ways.

Once a nation has decided upon its basic political and legal doctrines, it must address how it intends to defend their society and its chosen way of life. It is in military doctrine where the fundamental principles by which a country's military force guides its actions in support of national objectives [17]. Military doctrine can be segmented into fundamental, environmental, and organizational doctrines, which identify key military factors and addresses how each is to be governed and under what conditions. The nature of war, the purpose of military forces, and their relationship to other instruments of power reside in fundamental doctrine. It is relatively insensitive to political philosophy or changes in technology. The following examples are typical statements of fundamental doctrine [13]:

- 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 part of a CWD may include such statements as governing principles in developing environmental and organizational components.

It is the accumulative understandings about the deployment of military forces in a particular operating medium (i.e. sea, air, land and space power) that inhabit environmental doctrine [13]. In the case of a CWD, the environment is likely to reside in those realities connected to information technologies, computer networks and the physical infrastructures that support them. The organizational aspects will likely be adaptations of existing structures. Both environmental and organizational components will require additional consideration throughout the CWD development process.

3. Decision Making Considerations

The presumption of being able to include all aspects and details needed to formulate a CWD would be inappropriate for an endeavor of this scale without a serious consideration of a collaborative and discussion framework. What this section of the paper offers is a conceptual starting point for establishing the key questions that may be used to form the consensus basis of a CWD. In this section, we offer several key strategic decisions/questions that we believe are required for clarifying and enumerating a doctrine for cyber war. We offer these questions as critical examples of the types of queries needed to enable a corrective and decisive response when an attack does occur, and it is these types of queries that will form the foundation of Section 4 of this paper. Our proposed questions are as follows:

A. Determining the difference between traditional and cyber war

Definitions do matter when implementing policy and the choice of definition in developing a CWD must be done so with the help of a variety of input considerations. In essence, this question focuses on the role of information technology as an enabler of warfare and therefore its consideration as a viable target in both attack and defense viewpoints. The authors' perspective of cyber war is that it will have kinetic world effects meaning real damage to physical infrastructure directly and indirectly [18]. The notion that an information age war would be bloodless and sterile is challenged [19] by the reality that our digital infrastructures are integrated with our physical capabilities in order to sustain and support modern warfare. Information is the central element of commanding the conflict space and the infrastructure that allows the flow of information is equally important. From a strategic perspective, we must consider an opponent in a cyber war conflict as a system composed of a series of subsystems [20]. Each subsystem that supports and sustains the larger systems enables a country to focus its resources towards the conflict. The essential question before us is to what extent a cyber war conflict will encompass real world assets and leads to full scale war. Without a clear distinction between cyber war 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 this distinction and/or inclusion is crucial to this endeavor.

B. Battlespace determination

Controlling the conflict space is a central strategy in resolving military conflicts. But when a country seeks to do so, what exactly are its focused objectives? The authors' perspective is that cyber warfare involves keeping an opponent from knowing as much about itself while knowing everything about them during a conflict [21] while preventing an opponent from doing the same to its own forces. This knowledge battle rationally extends towards controlling a nation's own resources while rendering the resources of their opponent ineffective. Preventing the use or mobilization of resources is central to controlling the conflict space. In an ever increasing integrated and interdependent global economy, the implications can quickly escalate to encompass unforeseen consequences. Battle space dominance is likely to include a nation's information infrastructure as well as the information flowing through it on both sides of the conflict. We must also consider all the pathways and infrastructure between the two parties in a conflict as information infrastructures are now rarely symmetric. These third party pathways would likely 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 controlling it.

C. Aggression versus response

Waging a moral war is essential to sustaining it and we believe that a cyber war is no different. The authors' perspective is that a measured response to a cyber war attack requires deterrence and escalation levels [22]. In a conflict, the strategic objective is to cause enough of an opponent's

systems to change such that they adopt your objectives or make it impossible for them to mount an opposition [20]. In a retaliatory action aimed at deterring future attacks, a CWD should establish responses that cost the aggressor more than it would benefit from such attacks to encourage restraint. If a significant penalty beyond an incident is not established, escalating attacks are likely to continue. It is the proportionality of such responses that must be considered in order to maintain a moral response. An assessment of any attack must be accompanied with a suitable and corresponding response to maintain its moral justification when damages and/or casualties are incurred. Therefore, determining the range of responses to attacks is critical to responding responsibly and these must be in alignment with a nation's strategic security goals.

D. Victory conditions

War must be waged with a constant regard to the peace desired [11]. As with having a response and escalation policy, knowing what constitutes victory is essential to not over reaching in a CWD. Responses to aggression must consider taking possession of the opponent's strengths as well as destroying their armed power, and these must be done with regards to public opinion [23]. Levels of desired outcomes must be tied to any response to an attack. Depending on the severity of an attack, 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. Where an aggressor has the full support of the attacking country, the elimination of the attack infrastructure may be warranted and serves as another example of a victory condition. 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.

E. Required assets

A comprehensive understanding of what is needed to wage a cyber war is essential to creating the infrastructure to supporting a CWD. Identifying the dependencies a military force has regarding information technologies is tightly coupled with defining the needed assets. Modern militaries rely heavily on those systems that provide speed of command in order to achieve information superiority and the massing of effects. The result in the rapid foreclosure of enemy action and the shock of closely coupled events make network-centric operations a significant strategic advantage [24]. Assets that enable increased information richness, reach, and shared awareness are responsible for the transformation of improved awareness into collaborative planning and synchronized action [25]. Assets that provide for peacekeeping measures such as border management and verification activities play a role in threat awareness and removal [26]. The authors' perspective is that these assets and any suitable measures to defend and/or attack them must be identified to prevent a CWD from lacking the proper scope and depth when implemented.

F. Moderating responses

We live in a 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 geopolitical consequences of taking direct action in a cyber war, no CWD would hold substantive meaning to a nation's larger strategic national 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 those factors that would inhibit effective and decisive responses in any cyber war conflict. While there will undoubtedly be additional issues raised in the discussions forming a CWD, we believe the queries presented are representative in both depth and scope to illustrate the key elements that need to be considered in such an endeavor.

4. JOINT DISCOURSE STRUCTURE

Coming to a consensus in matters of distributive scale often requires a process of discussion and discourse to arrive at workable solutions. 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 be inclusive of its closest stakeholders. Drawing upon the past for guidance, the authors propose a collaborative and discussion framework that is similar to the one used by U.S. President Dwight Eisenhower in confronting the expansion of communism and the threat of nuclear war. This President believed that the best way to formulate national policy in a democracy was to assemble the best qualified people with opposing views and vigilantly listen to them debate each other on an issue [27]. This approach formed the foundations of Project Solarium and resulted in the creation of a doctrine to govern the Cold War that is still in effect today [28].

The authors' position regarding this collaborative framework is that there are several important fundamentals that need to be observed if such a venture is to be successful. The first of these is that a CWD initiative should be initiated and governed by top government officials, as we believe that executive government is in the best position to facilitate and coordinate such an endeavor. Second, the participants that will compose the subject matter experts should be delegates from civilian government, defense, security and professional organizations related to information technology such that a broad set of skilled stakeholders are represented in the problem formulation and solving processes. Third, the

project for creating a CWD should have a relatively short period of project time allocated so that participants must stay focused on the tasks at hand and not expand the range and scope of the mandate. Forth, the results of such an endeavor should be accepted by the nation's head of state and be widely published. It is this last step that is of critical priority for it is the dissemination of a CWD that establishes the new norms of conduct and the subsequent consequences for its 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 1, the head of state as the chief executive of a nation initiates the CWD collaboration process by identifying and selecting the primary stakeholders that have both a vested interest in any outcomes of a CWD and the expertise to offer substantive contribution towards the endeavor. These stakeholders are compartmentalized by those from the business community, various government branches and agencies, and professional organizations that can bring experience and expertise to the table. From within each of these selections, each organization would select delegates to represent them at a convention that will be charged with creating a key set of questions such as those contained in section 3. Once these questions have been jointly agreed upon, phase 2 would commence. From here, the questions would then be sent to the selected organizations in phase 1 for deliberation. Because knowledge is often held by unlikely participants and also because of the larger implications of a CWD, the authors strongly suggest that these hearings be held in public forums where their constituents may freely offer policy ideas in answering the key questions. Once assembled collectively by the participant organizations, these policy suggestions will form the basis of phase 3. In this phase, the business community, government branches and agencies, and professional organizations would jointly assemble before the nation's head of state and security council to present their ideas for answering the questions and be prepared to defend their proposals from any opposing viewpoints. The critical concept in this phase is that it is the areas of discourse that must be rigorously reviewed by all the participants. It would fall to the security council to assemble those policies that were common between the stakeholders as well as those policies that withstood rigorous examination by the all participants. A final document would be enumerated and presented for final ratification. The authors' believe that it is from the above process that a CWD would be created that has stakeholder buy-in and input, addresses the main concerns a nation would face in a cyber war confrontation, and permits decisive action with the backing of the nation state.

In summary, the proposed framework for the development of a national CWD is based on some major principles:

- Such a venture would be at the discretion of the Head of State regarding both initiating the CWD process as well as its final acceptance.
- The development of a CWD 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 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 into the public domain.

5. CONCLUSIONS

Advances in information technologies have reached a level of development and integration into modern societies that it may now be used to negatively influence the wellbeing of a nation. There are numerous examples available and several of these have been presented in this paper. Attacks on these systems and infrastructures may one day soon escalate into a full scale military conflict as a result. Whether such an incident is provoked by third-party cyber criminal activities or is state sponsored, it is prudent for civilian efforts to be prepared. In preparation, many defense forces are also developing and/or mobilizing themselves for future cyber war conflicts on a national and international level. To our knowledge to date, there is no comprehensive national strategy for handling a cyber war that brings the civilian infrastructure in alignment with military operations in a collaborative environment. In this paper, we have summarized many of the dominant issues required to formulate a comprehensive national CWD. We have outline a collaboration process towards this objective in order to bring together government, business and professional organizations that are responsible for a country's cyber infrastructure and national security.

REFERENCES

[1] Parrish, K., "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", Economist, July 1, 2010, available at http://www.economist.com.

[3] Stoll, C., The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, NY, Pocket Books, 1989.

[4] Alperovitch, D. Revealed: Operation Shady RAT, McAfee White paper, Publication No 33000, August 2011, available at http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[5] Molander, R., Riddle, A., Wilson, P., Strategic Information Warfare, A New Face of War. National Defense Research Institute RAND, 1996.

[6] Cybercrime, Cyberterrorism, Cyberwarfare, Averting an Electronic Waterloo, Washington, DC, Centre for Strategic and International Studies, 1998.

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

[8] "The National Strategy to Secure Cyberspace", Washington DC, US White House, 2003, available at: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

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

[10] "International Strategy for Cyberspace", Washington, DC, US White House, 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[11] Liddell-Hart, Basil Henry, Strategy: The Indirect Approach, (London, Faber and Faber Limited, Second revised edition, 1967.

[12] Webster's New World Dictionary and Thesaurus, Second Edition. Wiley and Sons, 2002.

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

[14] Tiller, E and Cross, F., "What is legal doctrine?", Northwestern University Law Review, Vol. 100, No. 1, 2006.

[15] The New Oxford American Dictionary, Second Edition. Oxford University Press, 2005.

[16] Kozel, R. "Stare Decisis as Judicial Doctrine", Washington and Lee Law Review, Vol. 67, No. 2, 2010.

[17] Department of Defense Dictionary of Military and Associated Terms, Joint Chiefs of Staff, Joint Publication 1-02, 8 November 2010.

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

[19] Sullivan, G and Dubik. J., War in the Information Age, Carlisle Barracks, Pa, US Army War College, 1994.

[20] Warden, J., "The Enemy as a System", Airpower Journal, Spring, 1995.

[21] Arquilla, J. and Ronfeldt, D., "The Advent of Netwar: Analytic Background", Studies in Conflict & Terrorism, No 22(3), 1999, pp.193-206.

[22] Tirenin, W. and Faatz, D. "A Concept for Strategic Cyber Defense", IEEE Military Communications Conference, Atlantic City, NJ, 1999.

[23] Clausewitz, C., On War, (originally London, N. Trübner, 1873, Translated and edited by Hans W. Gatzke, The Military Service Publishing Company, 1952.

[24] Cebrowski, A., "Network Centric Warfare: Its Origin and Future", Naval Institute Proceedings, 1998, pp.28-35.

[25] Alberts et al, Understanding Information Age Warfare, Washington, DC, CCRP Publication Series, 2001.

[26] Cahill, T., Rozinov, K., Mule, C., Cyber Warfare Peacekeeping, West Point, NY United States Military Academy, Proceedings of the 2003 IEEE Workshop on Information Assurance, June 2003, pp. 100-106.

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

[28] Eisenhower, D. Minutes of 155th Meeting of NSC, Papers as President, 1953-1961, NSC Series, Box 4, 1953.