REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE ***(DD-MM-YYYY)*** 27-10-2010	**2. REPORT TYPE** FINAL	**3. DATES COVERED** ***(From - To)***

4. TITLE AND SUBTITLE

Aggression in Cyberspace: Framing an Operational Response

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Douglas S. Coppinger, USAF

Paper Advisor: Colonel Thomas A. Heaney, Jr., USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations
Department
Naval War College
686 Cushing Road

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The rapid development of cyber-related technologies has outpaced the U.S. government's ability to create comprehensive cyber policy. Yet, if U.S. military commanders are expected to operate within the complex cyberspace environment, they require an operational framework to guide them. Whereas existing military frameworks are currently insufficient, the Information Operations Condition (INFOCON) system offers a potential baseline from which to create current guidance.

INFOCONs should, therefore, be broadened into a new system that addresses: the convergence of interdependent informational technology infrastructures; rule-based cyber engagement criteria and operational response thresholds; standing execution authorities; traditional risk acceptance and accountability techniques; and finally, response options integrating information assurance actions, defense actions, defense response actions, and offense actions. Once established, this new Cyber Condition (CYBERCON) system framework would be a suitable operational substitute for nonexistent cyberspace policy and would position military commanders to more effectively respond to aggressive events within cyberspace.

15. SUBJECT TERMS
Cyber, cyberspace, INFOCON, Information Operations

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		29	**19b. TELEPHONE NUMBER** ***(include area code)*** 401-841-3556

NAVAL WAR COLLEGE

Newport, R.I.

AGGRESSION IN CYBERSPACE: FRAMING AN OPERATIONAL RESPONSE

by

Douglas S. Coppinger

Lieutenant Colonel, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ___________________________

18 October 2010

Contents

Abstract

The rapid development of cyber-related technologies has outpaced the U.S. government‟s ability to create comprehensive cyber policy. Yet, if U.S. military commanders are expected to operate within the complex cyberspace environment, they require an operational framework to guide them. Whereas existing military frameworks are currently insufficient, the Information Operations Condition (INFOCON) system offers a potential baseline from which to create current guidance.

INFOCONs should, therefore, be broadened into a new system that addresses: the convergence of interdependent informational technology infrastructures; rule-based cyber engagement criteria and operational response thresholds; standing execution authorities; traditional risk acceptance and accountability techniques; and finally, response options integrating information assurance actions, defense actions, defense response actions, and offense actions. Once established, this new Cyber Condition (CYBERCON) system framework would be a suitable operational substitute for nonexistent cyberspace policy and would position military commanders to more effectively respond to aggressive events within cyberspace.

INTRODUCTION

> "One hacker, plus one modem causes an enemy damage and losses almost equal to those of a war. Because it has the breadth and secrecy of trans-level combat, this method of individual combat very easily achieves results on the strategic and even war policy levels." -- *Qiao Liang and Wang Xiangsui* [1]

In 1965, Intel© Corporation co-founder Gordon Moore accurately predicted that the number of transistors on a computer chip would double every two years. What lies at the heart of "Moore‟s Law," as it has since become known, is a broader recognition that cyber technology is undergoing a linear degree of growth and change. Noticeably missing, however, is a policy corollary to Moore‟s Law; one that keeps pace with how we are to leverage and apply these rapidly evolving technologies. Given the fact that technology development has outpaced our ability to develop guidance, military commanders are left particularly ill-prepared to respond to aggressive events within cyberspace. Since military commanders cannot rely on current guidance, they must have a ready framework in place to deal with both fleeting and enduring events of cyber aggression. While some legacy frameworks currently exist, they have not sufficiently evolved to deal with the ever-changing cyberspace environment. But one of these traditional structures does hold some future promise. The information assurance based construct that underpins the Information Operations Condition (INFOCONs) system is currently insufficient to frame an operational response to cyber aggression. However, were it to evolve into a broader network-based framework, combining information assurance responses with defensive actions, defense response actions, and offensive actions, military commanders would be effectively positioned to counter aggressive events in cyberspace, like the type of threat Qiao Liang and Wang Xiangsui described above.

BACKGROUND

The growth of information-related technologies over the past half-century has reached unprecedented levels, with worldwide installed personal computers (PCs) surpassing 1 billion units in June 2008,[2] an additional 308 million PCs shipped in 2009, and 368 million PCs projected to be shipped by the end of 2010.[3] While this technology has become more wide-spread, so has the associated user base, with the number of worldwide internet users surpassing 1 billion in December 2008.[4] This growth of information technologies, however, is not limited to PCs and the internet. The number of worldwide mobile phone subscriptions reached 4.6 billion in February 2010 and is expected to reach 5 billion by the end of the year.[5] As this growth continues unabated, it should not be surprising to realize among the enormity of the collective user base are bad actors intent on using this burgeoning technology for nefarious purposes.

In an appearance before Congress, General Kevin Chilton, Commander, U.S. Strategic Command, characterized these bad actors as ranging from "bored teenage hackers" to "the criminal element" to "the organized nation-state."[6] Along with the rising number and skills of bad actors is a commensurate increase in the number of DoD network intrusions.[7] It is estimated more than 100 foreign intelligence organizations[8] are specifically targeting our military networks, subjecting them to hundreds of thousands of probes every day.[9] Yet, it is precisely within this contested cyber battle space where military commanders are expected to routinely operate. As Raphael Perl, anti-terrorism lead for the Organization for the Security and Cooperation in Europe (OSCE) recently stated, "Make no mistake, in terms of anonymity in cyberspace, the responsible elements of society are in an ongoing arms-type race for the competitive technological edge with terrorists and criminals. And unfortunately, at this point in time, the good guys are not winning."[10]

So why, in this dynamic cyber environment, has the more time-honored military approach of deterrence failed to discourage the behaviors of these bad actors? In a word: attribution. Unlike the telephone system, the internet was not designed with a requirement to determine the identity of an end user. Telephony networks were conceived with a need to charge end users a fee for service, so the system intentionally contained mechanisms to track and bill users each time the networks were accessed. The internet, on the other hand, was developed as a collaborative system with the expressed purpose of sharing of ideas and information. No need was envisioned, nor provisions made, to track or identify end users.[11] Thus, it is relatively easy to operate anonymously within cyberspace.

Attribution is not the principal challenge posed by the inherent nature of cyberspace since speed similarly complicates the environment. Cyberspace transmissions occur at a rate approaching the speed-of-light. When considered within the context of the interconnectivity of networks, cyber attacks appear quickly and spread quickly. The 2010 National Strategy to Secure Cyberspace documented two such attacks; one that went "from nonexistent to nationwide in an hour, lasted for days, and attacked 86,000 computers," and a second that infected 150,000 computer systems in 14 hours.[12] Therefore, operational decision cycles and responses must be equally rapid. Regrettably, a lack of current policy and guidance impedes a military commander"s ability to quickly respond.

Back in October 2003 when the DoD Information Operations (IO) Roadmap was published, it acknowledged, "A review of existing policy for IO found that policy lags behind operations" and further amplified, "Computer Network Defense (CND) lacks up to date policy and legal guidance…to guide response to intrusions or attacks on DoD networks."[13] Seven years later this policy gap has yet to be bridged. In April 2010, Senator Carl Levin, stated "capabilities to operate in cyberspace have outpaced the developing of policy, law, and precedent to guide and control those operations,"[14] and General Keith Alexander echoed, "President Obama‟s cyber security sixty-day study highlighted the mismatch between our technical capabilities to conduct operations and the governing laws and policies."[15] This inability to create current cyber policy suggests the rate of modern technological change has simply overwhelmed traditional policy creation mechanisms.

Therefore, if military commanders are expected to successfully operate within a cyberspace environment characterized by anonymity and speed, but absent policy, they require a ready framework that lends itself to compressed timelines and rapid decision cycles to guide their actions. The Information Operations Condition (INFOCON) system may be just such a framework.

DISCUSSION/ANALYSIS

Prior to 2006, the INFOCON system was, according to Department of Defense Instruction O-8530.2 "a comprehensive defensive posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent." This well-structured approach was specifically designed to defend against attacks on friendly information systems.[16] Apparently modeled after the Defense Readiness Condition (DEFCON) system, the INFOCON system was divided into five incremental threat levels designed to balance our information systems‟ defensive postures against perceived threats.[17] However, as a Microsoft Corporation executive recognized, "Most computer security experts believe that a well-resourced and persistent adversary will more often than not be successful in attacking systems, especially if raising defenses is the only response to an attack."[18]

So, in 2006, the INFOCON system shifted focus away from a reactive, threat-based model to what was termed a proactive, readiness-based approach.[19] This new INFOCON system was based on the realization that networks were impossible to completely safeguard. Accepting network intrusions as an inevitability led to a new methodology that emphasized “returning the system to a pristine, baseline state” in order to “restore confidence in the system.”[20]

According to Strategic Command Directive (SD) 527-1, this improved Information Operations Condition system approach was designed to provide a mechanism for commanders to match the readiness of their networks with operational priorities. As commanders maneuvered among the five INFOCON levels and tailored response options, the method and frequency of information assurance activities changed to increase the commander‟s confidence in the information systems.[21] Table I below depicts the current INFOCON levels, the predominant activities associated with each level, and the categorized tailored response options available to commanders. [22]

TABLE I

Information Operations Conditions (INFOCONs)		**Tailored Response Options (TROs)**	
INFOCON 5	Maintain accurate system baselines	TRO 1 – Passwords	TRO 6 – Intrusion Detection System rules
INFOCON 4	Regularly validate known good image of information network against its current state	TRO 2 – Rebuilding key servers	TRO 7 – Access Control Lists
INFOCON 3	Increase frequency of validating information network	TRO 3 – Permissions	TRO 8 – Connectivity
INFOCON 2	Further increase in frequency of validating information network	TRO 4 – Anti-virus definitions	TRO 9 – Logging
INFOCON 1	Reload operating system software on key servers	TRO 5 – Firewall signatures	TRO 10 – Load Control

Despite the systemic changes that occurred in 2006, there are three major deficiencies that sub optimize the utility of the current INFOCON system: the name, the response, and the network.

The name. Examining the actions taken at each INFOCON system level, as well as the categories of the TROs, reveals an apparent theme: they are fundamentally information assurance based despite the fact that these are purportedly "Information Operations" conditions versus "Information Assurance" conditions. This distinction holds greater significance than the mere parsing of a naming convention suggests.

Information assurance is defined as "information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation."[23] As stated above, information assurance is not in and of itself information operations; it is instead a fractional subset of information operations. Hierarchically, information assurance is a subset of computer network defense (CND) actions. CND is itself a subset of computer network operations (CNO). CNO, ultimately, is one of the five activities that combine to form information operations.

By definition, "Information operations is distinguished from information assurance in that it does not apply to the entire information systems life cycle. Rather, it represents operations that employ CND with other activities such as military deception, psychological operations and electronic warfare to affect or defend information and information systems and contribute to achieving information superiority."[24] If the INFOCON system was truly based on information operations, then it would harmonize information assurance techniques like those listed within Table I, along with the other activities that form information operations: military deception

(MILDEC), operational security (OPSEC), psychological operations (PSYOP), electronic warfare (EW), and computer network operations (CNO). Since the INFOCON system fails to incorporate broader information operations activities, by name the INFOCON system is incomplete.

The response. A second discrepancy within the INFOCON system is its failure to include actions directed against the cyber aggressor. As currently written, the military operational response within this system is limited to ensuring friendly information networks are inviolate.

The DoD Information Operations Roadmap of 2003 correctly points out that the "DoD requires a robust, layered defense across the Department based on global and enclave situational awareness with a centralized capability to rapidly characterize, attribute and respond to attacks." This strategy, termed "defense in depth," presumes the need to "fight the net" much like any other DoD weapon system.[25] So, in theory the strategy is one of defense in depth. In practice, the INFOCON system self-limits to a fractional, information assurance portion of a defense. Therefore, it represents an incomplete defense without depth.

A comprehensive, in-depth defensive strategy should not be restricted to defensive actions alone. A bastion-type defense of building higher and thicker firewalls, for example, would have negligible impact on a determined aggressor. A layered defense should include active defenses, known as defense response actions. This would allow a defender to take counteractions against a cyber aggressor. These active defenses should play a pivotal role, "paramount in which the attacker is forced to pay a price for targeting a system."[26]

Finally, defense in depth should not be perceived as an exclusively defensive undertaking. The IO Roadmap describes defense in depth as integrating offensive capabilities as well.[27] As recently as April 2010, Senator John McCain commented, “Continuing intrusions and attacks by difficult to identify and locate actors on our civilian and military networks and web sites demand not only a robust defensive capability, *but the ability to respond offensively* when the circumstances call for it [emphasis added].”[28] Even our National Military Strategy for Cyberspace Operations assesses, “operations are strongest when offensive and defensive capabilities are mutually supporting.”[29] Therefore, the information assurance based INFOCON system is insufficiently nested within the broader “defense in depth” strategy since it fails to integrate defensive actions, defense response actions, and offensive actions.

The network. The third major deficiency regarding the INFOCON system involves information networks. The INFOCON system has evolved to address the readiness of a commander‟s networks. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as “the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”[30] Thus, if networks are interdependent, as the definition of cyberspace suggests, then precisely which network(s) should the INFOCON system apply to?

The Director of National Intelligence (DNI) was quoted in the 2009 White House Cyberspace Policy Review as attesting, “the growing connectivity between information systems, the internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and general critical infrastructure protection.”[31] What the DNI is addressing is the convergence of traditional information networks with other networks. For example, with the advent of smart phone technology and the widespread use of BlackBerrys and iPhones, the distinction between what constitutes a traditional information network (i.e. computer and/or internet) and a traditional telephony network is becoming increasingly blurred. However, each of these networks is, at its core, an information network and each requires protection. The current INFOCON system, though, is specifically designed to address the more traditional information networks of computer and internet, ignoring the convergence of other informational technology infrastructures. Therefore, the INFOCON construct in place since 2006 has failed to adapt to the changes within and among the very networks it was originally intended to protect.

Overall, the rapid development of information technology infrastructures has simply outpaced the ability of the INFOCON system to function as designed. The discrepancies noted with the name, response, and network of the INFOCON system indicate a structure that is obsolescing. In its present state, it is an insufficient substitute for a military commander to use in place of nonexistent cyber policy. However, the current INFOCON system model could be used as the foundation from which to build a future system; one that addresses the aforementioned discrepancies and provides a comprehensive framework to guide a military commander"s actions in cyberspace.

Whereas a finely detailed description of an INFOCON replacement system would exceed the classification of this monograph, there are certain general characteristics that a substitute framework must address. Those characteristics include: broader inclusivity, rule-based engagement criteria, standing execution authorities, integrated response options, and risk acceptance and accountability.

Broader inclusivity. Due to the decreasing distinction between types of networked information systems, the Information Operations Conditions (INFOCON) system should be replaced with one that addresses the convergence of information networks. A Cyber Condition (CYBERCON) system would take into account information system technologies at the broadest level. The CYBERCON system‟s function should be equally expanded to include truly proactive risk, readiness, and response levels to account for the operational environment, friendly network postures, and the characterization of actions taken in response to the current environment. Each level of this system would, by definition, provide a more complete picture of the risk, readiness, and response of a commander‟s information networks than the current INFOCON system (see Table II).

TABLE II

CYBERCON SYSTEM			
Level	Risk	Readiness	Response
CYBERCON 5	Normal activity	Maintain accurate system baselines	Emphasizes IA actions
CYBERCON 4	Increased risk/incidents of disruptions, intrusions or attack	Regularly validate known baseline image of information network against its current state	Emphasizes IA and defensive actions
CYBERCON 3	Specific risk/incidents of disruptions, intrusions or attack	Increase frequency of validating information network	Emphasizes defensive actions. Defense response actions are authorized and may be appropriate
CYBERCON 2	Limited disruptions, intrusions or attack	Further increase in frequency and method of validating information network	Emphasizes defensive, and defense response actions. Offensive actions are authorized and may be appropriate
CYBERCON 1	General disruptions, intrusions or attack	Reload operating system software on key servers	Emphasizes defensive, defense response actions, and/or offensive actions[32]

Rule-based engagement criteria. Since military organizations are familiar with standing rules of engagement, an improved framework would minimally address the following standing rule sets: under what event-based conditions are cyberspace engagements authorized; how specific cyberspace response options are affected by the scope, duration, and impact (intended and/or actual) of the attack/aggression/intrusion; and finally, what limitations in terms of scope, duration, and impact are placed on the military‟s operational cyberspace response.[33] While these rule sets could appear as a conditional matrix (if/then syntax), the specific format is less important than the fact that the impact of each of these issues has been thoughtfully considered and addressed in advance. An effective rule set should provide the commander a ready reference outlining the range of allowable response options resulting from network events. Establishing conditional threshold criteria in advance should compress decision cycles and increase the speed of a military commander‟s operational response.

Standing execution authorities and capabilities. Due to the characteristically rapid nature of cyberspace events, the sometimes fleeting nature of a response window, and the difficulty of a traditional command and control (C2) structure to react to a highly compressed timeline, delegated cyber capabilities and pre-existing execution authorities should be bundled within each level of the CYBERCON framework. [34] This could be accomplished by establishing dynamic toolkits composed of tested and validated capabilities (e.g. tools, tactics, techniques, and procedures) optimized to emphasize appropriate response actions at each CYBERCON level. A failsafe mechanism should also exist for the commander to request additional capabilities or response options not specifically authorized under the standing execution authorities.[35] Overall, these pre-packaged authorities and capabilities would give military commanders a menu of flexible response options to address cyberspace aggressions as they occur.

Integrated response options. As described within a recent white paper, "While there is a great need to harden DoD infrastructure from these attacks, passive computer network defenses cannot be, and will never be, perfect. Thus, if the DoD attempts to passively withstand all attacks, it will eventually succumb to a serious attack. As with conventional warfare, a good offense is often the strongest defense."[36] Therefore, individual CYBERCON system levels should be designed to include appropriate capabilities as they relate to information assurance actions, defensive actions, defense response actions, and/or offensive actions, as required. Since CYBERCONs are based on risk, readiness, and response, specific emphasis will vary according to each CYBERCON level. Level-specific toolkits should be structured to represent the emphasized actions. For example, the CYBERCON 5 toolkit would emphasize information assurance capabilities, but would contain broader, in-depth defense capabilities. The CYBERCON 4 toolkit would incorporate the CYBERCON 5 toolkit, but would add more robust defensive capabilities, as well as broader defense response action capabilities. Since CYBERCON 1 represents the greatest risk, its toolkit would be the most expansive and would include sensitive offensive capabilities. Finally, the response options within the CYBERCON system would not be prescriptive, but rather a range of integrated capabilities immediately available for discretionary use by military commanders.

Risk acceptance and accountability. The National Strategy to Secure Cyberspace appropriately noted, "…consideration should be given to the broad-based costs and impacts of a given government action, versus other alternative actions, versus non-action…."[37] Military commanders should, similar to operations within other domains, accept risk and be held accountable for their actions or non-action in cyberspace.[38] Whereas risk acceptance and accountability are implicit in other domains, the CYBERCON framework should explicitly address risk as it applies to ambiguous attribution. Specifically, during times of cyber aggressor ambiguity, military commanders should be authorized to operationally respond if, after weighing the risk, they perceive the benefits of action outweigh the perceived cost.[39]

To synthesize the previously described characteristics of a new CYBERCON system, consider the following scenario: A military commander is operating in CYBERCON 5. A network intrusion occurs that trips the conditional, rule-based engagement criteria threshold requiring the commander to declare CYBERCON 3. Upon declaration, the commander has standing execution authority to immediately respond to the intrusion using the prepackaged capabilities contained within the cyber toolkit designated specifically for CYBERCON level 3. From this toolkit, the commander determines which and how individual capabilities will be harmonized and employed in response to the intrusion. Should the commander desire a capability not in the toolkit, it can be requested. However, the commander must balance the value of the desired capability versus the time required for the submission of, and response to, the request. Due to the nature of the CYBERCON 3 event, the commander would likely emphasize a blocking maneuver to prevent further harm to the network (defensive actions), then consider engaging the source or method of the intrusion, if appropriate (defense response actions), and finally, ensure the integrity of the friendly network (information assurance actions). Ultimately, the commander assumes the risk and accountability for actions taken in response to declaring CYBERCON 3.

Within the above scenario, the CYBERCON system addresses: risk, by raising the threat posture to level 3; readiness, through ensuring the integrity of the friendly network; and response, through defensive and defense response actions. In application, this CYBERCON system would allow a military commander to more completely respond to cyber aggressions as compared to any existing framework.

COUNTERARGUMENTS

Since the legality of military use of cyberspace is not well established, some could argue the current INFOCON framework, which restricts responses to information assurance actions, already operates at the limits of propriety. However, as General Keith Alexander recently testified, “a commander‟s right to self-defense is clearly established in both U.S. and international law. Although this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with law of war principles (e.g. proportionality), would be lawful.” [40]

Others argue discretionary rules of engagement for self-defense, “could be rarely exercised in cyberspace, if ever, since a counterstrike in cyberspace is likely to lack clear attribution and clear scoping of the side effects on neutral parties.”[41] Yet, self-defense actions have never been contingent on positively identifying an aggressor. Again, General Keith Alexander is on record stating, “…circumstances may be such that at least some level of mitigating action can be taken even when we are not certain who is responsible. Regardless, whether we know who is responsible, international law requires that our use of force in self-defense be proportional and discriminate. Neither proportionality nor discrimination requires that we know who is responsible before we take defensive action.”[42]

To clarify, he described two analogous scenarios. In the first, he focused on the attacker, and stated it was not necessary for a policeman to establish the identity of the individual shooting at them in order to shoot back. In the second, he focused on the method of the attack, and described “someone in a car trying to run down a police officer.” In this scenario, he indicated the police officer would “not be required to determine whether the car is stolen before shooting out the tires in self-defense. Similarly, the fact that computers may be commandeered is irrelevant to the exercise of self-defense.”[43]

The common thread within both of the aforementioned arguments involves the limits imposed on military operations in cyberspace. Since existing laws are somewhat ambiguous, the U.S. should earnestly contemplate establishing a “declaratory policy” on how cyberspace will be viewed and used. This concept has been previously suggested within the Department of Defense,[44] as well as within the private sector, [45] but has failed to gain sufficient traction. An advantage offered by a declaratory policy would be to provide clarity to other nations, bad actors and military commanders alike on how the U.S. intends to operate within this complex cyberspace domain. The rule-based engagement criteria previously described within the CYBERCON system framework would complement this declaratory policy, but would not be dependent on the existence of such a policy to function.

A consideration within any declaratory policy would be the need to delineate when network intrusions would be viewed as acts of war. As Anders Fogh Rasmussen, NATO‟s secretary-general, recently recognized, “It‟s no exaggeration to say that cyber attacks have become a new form of permanent, low-level warfare.”[46] By accepting that penetrations of friendly networks do not occur by accident, but with malice of forethought, the U.S. government would be well served to declare conditions whereby network intrusions would be treated as warfare, and therefore, demand operational responses consistent with law of war principles, even during peacetime.

Absent any declaratory policy, military commanders continue to possess an inherent right to self-defense. Under the provisions of self-defense, and limited to law of war principles, current laws support operational responses to acts of cyber aggression. While an inability to confirm the identity of an attacker or precise ownership of the method of an attack may complicate response considerations, they do not preclude a military commander from initiating an operational response. Therefore, without any change to existing law, and lacking any declaratory policy, military operations in and through cyberspace remain legally justifiable.

CONCLUSIONS AND RECOMMENDATIONS

Military commanders currently find themselves operating within a contested battle space without a ready means to respond to aggressive actions. The sheer volume of attempted network intrusions, along with the inherent difficulty in attributing those aggressive events to specific bad actors, aggravates the challenges posed by a lack of comprehensive cyber policy. Further complicating this already complex environment is the speed at which attacks are carried out and the corresponding speed required to respond. Yet, operational commanders must be appropriately positioned and sufficiently equipped to act.

Just as cyber policy has failed to keep pace with evolving technological developments, existing operational frameworks have likewise obsolesced. In particular, the inappropriately named "Information Operation" Condition system, limited in response actions and narrow in scope, should be abandoned in its current form and redesigned to build a future, more inclusive, operational framework.

A future system constructed around the INFOCON model should include a broader definition of information networks in order to account for the increasing network convergences, as well as the interconnectivity of today‟s information systems. This new CYBERCON system should also specify predetermined operational risk, readiness, and response levels. Rule-based engagement criteria should identify discrete conditions and thresholds that would trigger an operational response. Standing execution authorities would also be required in order to account for the compressed timelines associated with operational decision cycles and responses. Individual CYBERCON levels would need to include a range of military response options that fully integrate information assurance actions, defense actions, defense response actions, and offense actions, as appropriate. Finally, traditional risk acceptance and accountability would be maintained at the military operational commander level, just as it is within more traditional domains.

While not essential to implementing the recommended CYBERCON system, establishing a declaratory policy would serve to affirm how the U.S. government intended to view and use cyberspace. This policy would clarify when network intrusions would be deemed an act of warfare demanding operational responses consistent with law of war principles.

Even without a complementary declaratory policy, the proposed CYBERCON system complies with existing laws and should serve to bridge the gap between nonexistent cyberspace policy and military operations within cyberspace. As described, this operational framework would, for the first time, provide military commanders a comprehensive range of flexible response options to effectively counter aggressive events within cyberspace.

NOTES

[1] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, China: PLA Literature and Arts Publishing House, 1999), 199.

[2] Gartner, "Gartner Says More than 1 Billion PCs In Use Worldwide and Headed to 2 Billion Units by 2014," *Gartner.com*, 23 June 2008, http://www.gartner.com/it/page.jsp?id=703807/ (accessed 20 September 2010).

[3] Gartner, "Gartner Says Worldwide PC Shipments to Increase 19 Percent in 2010 with Growth Slowing in Second Half of the Year," *Gartner.com*, 31 August 2010, http://www.gartner.com/it/page.jsp?id=1429313/ (accessed 20 September 2010).

[4] Mark Hachman, "Internet Users Top 1 Billion, Most of Them Asian," *PCMag.com*, 26 January 2009, http://www.pcmag.com/article2/0,2817,2339592,00.asp/ (accessed 20 September 2010).

[5] Associated Press, "Number of Cell Phones Worldwide Hits 4.6B," *CBSNews.com*, 15 February 2010, http://www.cbsnews.com/stories/2010/02/15/business/main6209772.shtml/ (accessed 20 September 2010).

[6] Paul A. Matus, "Strategic Impact of Cyber Warfare Rules for the United States," (Strategic Research Project, Carlisle Barracks, PA: U.S. Army War College, 2010), 4, http://www.dtic.mil/sgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522001/ (accessed 22 August 2010).

[7] Redacted version of classified document. U.S. Department of Defense, *Information Operations Roadmap,* (Department of Defense, Washington, DC: DoD, 30 October 2003), 44-45, http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[8] Ellen Nakashima, "U.S. Cyber-Security Strategy Yet to Solidify," *Washington Post*, 17 September 2010, http://ebird.osd.mil/ebfiles/e20100917776113.html/ (accessed 17 September 2010).

[9] Senate, *Nominations of VADM James A. Winnefeld, Jr., U.S. Northern Command/Commander, North American Aero-Space Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*, 111th Cong., 2nd sess., 2010, 17.

[10] Raphael Perl, "Combating Terrorist Use of the Internet/Comprehensively Enhancing Cyber Security," (Remarks, 2010 Counter Terror Expo, London, UK, 14 April 2010), http://www.osce.org/documents/atu/2010/04/43495/ (accessed 29 August 2010).

[11] Dr. Jeffrey Hunker, Bob Hutchinson, and Jonathan Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution,* (I3P Report, Hanover, NH: Institute for Information Infrastructure Protection, 2008), 5-6.

[12] U.S. President. *The National Strategy to Secure Cyberspace*, (Washington, DC: White House, 2003), 6, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf/ (accessed 21 September 2010).

[13] Department of Defense, *Information Operations Roadmap,* Department of Defense (Washington, DC: DoD, 30 October 2003), 18. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[14] Senate, *Nominations of VADM James A. Winnefeld, Jr., U.S. Northern Command/Commander, North American Aero-Space Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*, 111th Cong., 2nd sess., 2010, 3.

[15] Washington Post, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," *Washington Post*, 14 April 2010, 9, http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf/ (accessed 30 August 2010).

[16] Department of Defense, *Support to Computer Network Defense (CND),* Department of Defense Instruction O-8530.2. (Washington, DC: DoD, 9 March 2001), 22.

[17] Ibid., 22.

[18] Scott Charney, "Rethinking the Cyber Threat: A Framework and Path Forward, " (White Paper, Redmond, WA: Microsoft Corporation, 2009), 5, http://www.microsoft.com/downloads/details.aspx?FamilyID=062754CC-BE0E-4BAB-A181-077447F66877&amp;displaylang=en&displaylang=en/ (accessed 28 August 2010).

[19] U.S. Strategic Command, *Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures,* Strategic Command Directive (SD) 527-1 (Offutt AFB, NE: U.S. Strategic Command, 27 January 2006), 5, http://publicintelligence.net/strategic-command-directive-sd-527-1/ (accessed 30 August 2010).

[20] Ibid., 5.

[21] Ibid., 5.

[22] Ibid., 29-30.

[23] Department of Defense, *Computer Network Defense (CND),* Department of Defense Directive O-8530.1. (Washington, DC: DoD, 8 January 2001), 13.

[24] Department of Defense, *Support to Computer Network Defense (CND),* Department of Defense Instruction O-8530.2. (Washington, DC: DoD, 9 March 2001), 17.

[25] Department of Defense, *Information Operations Roadmap,* Department of Defense (Washington, DC: DoD, 30 October 2003), 13. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[26] Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law" (J.D. paper, Stanford, CA: Stanford Law School, 2008), 13, http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf/ (accessed 23 August 2010).

[27] Department of Defense, *Information Operations Roadmap,* Department of Defense (Washington, DC: DoD, 30 October 2003), 46. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[28] Senate, *Nominations of VADM James A. Winnefeld, Jr., U.S. Northern Command/Commander, North American Aero-Space Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*, 111th Cong., 2nd sess., 2010, 4.

[29] Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: Department of Defense, 2006), 10. Redacted version of classified document.

[30] Melissa Hathaway, *The Cyberspace Policy Review,* (Washington, DC: White House, 2009), 1, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 21 September 2010).

[31] Ibid., 3.

[32] The CYBERCON risk descriptors are based upon, but modified by author, from the pre-2006 INFOCON descriptors. The CYBERCON readiness descriptors are based upon, as interpreted by author, the current INFOCON-prescribed actions. Department of Defense, *Computer Network Defense (CND),* Department of Defense Directive O-8530.1. (Washington, DC: DoD, 8 January 2001), 13.

[33] Author-modified considerations as suggested and/or inspired by William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academies Press, 2009), 169.

[34] As suggested within the IO Roadmap, Combatant Commanders should be given the capabilities and selected execution authorities required to rapidly employ IO capabilities. Department of Defense, *Information Operations Roadmap,* Department of Defense (Washington, DC: DoD, 30 October 2003), 12, 23. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[35] According to Melissa Hathaway, "Answering the question of „who is in charge" must address the distribution of statutory authorities and missions across departments and agencies. This is particularly the case as telecommunications and internet-type networks converge and other infrastructure sectors adopt the internet as a primary means of interconnectivity." Melissa Hathaway, *The Cyberspace Policy Review,* (Washington, DC: White House, 2009), 4, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 21 September 2010).

[36] David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, (IDA Paper, Alexandria, VA: Institute for Defense Analysis, 2003), 2.

[37] U.S. President. *The National Strategy to Secure Cyberspace*, (Washington, DC: White House, 2003), ix, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf/ (accessed 21 September 2010).

[38] Chairman, U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, (Washington, DC: Department of Defense, 2006), F-3. Redacted version of classified document.

[39] U.S. President. *The National Strategy to Secure Cyberspace*, (Washington, DC: White House, 2003), 14, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf/ (accessed 21 September 2010).

[40] Washington Post, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," *Washington Post*, 14 April 2010, 24, http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf/ (accessed 30 August 2010).

[41] James Andrew Lewis, The "Korean" Cyber Attacks and Their Implications for Cyber Conflict, *Center for Strategic and International Studies,* (23 October 2009): 4. http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf/ (accessed 27 August 2010).

[42] Washington Post, "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command," *Washington Post*, 14 April 2010, 12, http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf/ (accessed 30 August 2010).

[43] Ibid., 24.

[44] Department of Defense, *Information Operations Roadmap,* Department of Defense (Washington, DC: DoD, 30 October 2003), 51. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

[45] Ellen Nakashima, "U.S. Cyber-Security Strategy Yet to Solidify," *Washington Post*, 17 September 2010, http://ebird.osd.mil/ebfiles/e20100917776113.html/ (accessed 17 September 2010).

[46] Siobhan Gorman and Stephen Fidler, "Cyber Attacks Test Pentagon, Allies and Foes," *Wall Street Journal,* 25 September 2010, http://ebird.osd.mil/ebfiles/e20100925777570.html/ (accessed 27 September 2010).

SELECTED BIBLIOGRAPHY

Associated Press. “Number of Cell Phones Worldwide Hits 4.6B.” *CBSNews.com*, 15 February 2010. http://www.cbsnews.com/stories/2010/02/15/business/main6209772.shtml/ (accessed 20 September 2010).

Charney, Scott. “Rethinking the Cyber Threat: A Framework and Path Forward.” White Paper, Redmond, WA: Microsoft Corporation, 2009. http://www.microsoft.com/downloads/details.aspx?FamilyID=062754CC-BE0E-4BAB-A181-077447F66877&amp;displaylang=en&displaylang=en/ (accessed 28 August 2010).

Chilton, Kevin, General, and Greg Weaver. “Waging Deterrence in the Twenty-First Century,” Strategic Studies Quarterly, Spring (2010): 31-42.

Gartner. “Gartner Says More than 1 Billion PCs In Use Worldwide and Headed to 2 Billion Units by 2014.” *Gartner.com*, 23 June 2008. http://www.gartner.com/it/page.jsp?id=703807/ (accessed 20 September 2010).

Gartner. “Gartner Says Worldwide PC Shipments to Increase 19 Percent in 2010 with Growth Slowing in Second Half of the Year.” *Gartner.com*, 31 August 2010. http://www.gartner.com/it/page.jsp?id=1429313/ (accessed 20 September 2010).

“Gates: Cyber Attack a Constant Threat.” *CBSnews.com*, 21 April 2009. http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml/ (accessed 21 August 2010).

Gorman, Siobhan and Stephen Fidler. “Cyber Attacks Test Pentagon, Allies and Foes.” *Wall Street Journal,* 25 September 2010. http://ebird.osd.mil/ebfiles/e20100925777570.html/ (accessed 27 September 2010).

Gorman, Siobhan, Yochi J. Dreazen, and August Cole. “Insurgents Hack U.S. Drones.” Wall Street Journal Online, 17 December 2009. http://online.wsj.com/article/SB126102247889095011.html/ (accessed 28 August 2010).

Graham, David E. Cyber Threats and the Law of War. *Journal of National Security Law & Policy*, vol. 4, no. 1 (2010): 87-102. http://www.jnslp.com/read/vol4no1/07_Graham.pdf/ (accessed 27 August 2010).

Hachman, Mark. “Internet Users Top 1 Billion, Most of Them Asian.” *PCMag.com*, 26 January 2009. http://www.pcmag.com/article2/0,2817,2339592,00.asp/ (accessed 20 September 2010).

Harknett, Richard J., and James A. Stever. "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen." *Journal of Homeland Security and Emergency Management*, vol. 6, issue 1, art. 79 (2009). http://www.bepress.com/jhsem/vol6/iss1/79/ (accessed 28 August 2010).

Harknett, Richard J., John P. Callaghan, and Rudi Kauffman. "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management*, vol. 7, issue 1, art. 22 (2010): 1-24.

Hathaway, Melissa. *The Cyberspace Policy Review*. Washington, DC: White House, 2009. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 21 September 2010).

Hunker, Dr. Jeffrey, Bob Hutchinson, and Jonathan Margulies. *Role and Challenges for Sufficient Cyber-Attack Attribution*. I3P Report. Hanover, NH: Institute for Information Infrastructure Protection, 2008.

Lewis, James Andrew. The "Korean" Cyber Attacks and Their Implications for Cyber Conflict. *Center for Strategic and International Studies* (23 October 2009): 1-10. http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf/ (accessed 27 August 2010).

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare*. Beijing, China: PLA Literature and Arts Publishing House, 1999.

Matus, Paul A. "Strategic Impact of Cyber Warfare Rules for the United States." Strategic Research Project, Carlisle Barracks, PA: U.S. Army War College, 2010. http://www.dtic.mil/sgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA522001/ (accessed 22 August 2010).

Mordente, Patrick, Paul Needham, and Theodore P. Ogren. "Logistics for the 21st Century: Deployment Distribution Operations Center, Quick Fix or Long-Term Solution?" Air Force Journal of Logistics, Winter 2006/Spring 2007, vol. 4, issue 1 (2007).

Nakashima, Ellen. "NSA director to testify at Senate hearing on cyber command unit." *Washington Post*, 14 April 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/04/AR2010041404013_pf.html/ (accessed 21 August 2010).

Nakashima, Ellen. "U.S. Cyber-Security Strategy Yet to Solidify." *Washington Post*, 17 September 2010. http://ebird.osd.mil/ebfiles/e20100917776113.html/ (accessed 17 September 2010).

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press, 2009.

Perl, Raphael. "Combating Terrorist Use of the Internet/Comprehensively Enhancing Cyber Security." Remarks. 2010 Counter Terror Expo. London, UK, 14 April 2010. http://www.osce.org/documents/atu/2010/04/43495/ (accessed 29 August 2010).

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Columbia Journal of Transnational Law*, vol. 37 (1999). http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA471993/ (accessed 25 August 2010).

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." J.D. paper, Stanford, CA: Stanford Law School, 2008. http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf/ (accessed 23 August 2010).

U.S. Congress. House. *Planning for the Future of Cyber Attack Attribution: Hearing before the Subcommittee on Technology and Innovation of the Committee on Science and Technology*. 111th Cong., 2nd sess., 2010.

U.S. Congress. House. *Untangling Attribution: Moving to Accountability in Cyberspace: Hearing before the Subcommittee on Technology and Innovation of the Committee on Science and Technology*. 111th Cong., 2nd sess., 2010.

U.S. Congress. Senate. *Nominations of VADM James A. Winnefeld, Jr., U.S. Northern Command/Commander, North American Aero-Space Defense Command; and LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Chief, Central Security Service/Commander, U.S. Cyber Command*. 111th Cong., 2nd sess., 2010.

U.S. Department of Defense. *Computer Network Defense (CND).* Department of Defense Directive O-8530.1. Washington, DC: DoD, 8 January 2001.

U.S. Department of Defense. *Information Operations Roadmap.* Department of Defense. Washington, DC: DoD, 30 October 2003. Redacted version of classified document. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf/ (accessed 10 September 2010).

U.S. Department of Defense. *Support to Computer Network Defense (CND).* Department of Defense Instruction O-8530.2. Washington, DC: DoD, 9 March 2001.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *The National Military Strategy for Cyberspace Operations*. Washington, DC: Department of Defense, 2006. Redacted version of classified document.

U.S. President. *The Comprehensive National Cybersecurity Initiative*. Washington, DC: White House, 2009. http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf/ (accessed 21 September 2010).

U.S. President. *The National Strategy to Secure Cyberspace*. Washington, DC: White House, 2003. http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf/ (accessed 21 September 2010).

U.S. Strategic Command. Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures. Strategic Command Directive (SD) 527-1.Offutt AFB, NE: U.S. Strategic Command, 27 January 2006. http://publicintelligence.net/strategic-command-directive-sd-527-1/ (accessed 30 August 2010).

Washington Post. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." *Washington Post*, 14 April 2010. http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf/ (accessed 30 August 2010).

Weinberger, Sharon. "Researchers Seek DNA of Cyber-Attacks." *Aviation Week*, 5 May 2010. http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=dti&id=news/dti/2010/05/01/DT_05_01_2010_p18-218207.xml/ (accessed 24 August 2010).

Westby, Jody R. "Cyber War v. Cyber Stability." Paper for the 42nd Session, World Federation of Scientists, Erice, Italy: International Seminars on Planetary Emergencies, 2009. http://www.globalcyberrisk.com/pdfs/WFS-Cyber-Stability.pdf/ (accessed 22 August 2010).

Wheeler, David A., and Gregory N. Larsen. *Techniques for Cyber Attack Attribution*. IDA Paper. Alexandria, VA: Institute for Defense Analysis, 2003.