2010-03

A legal reasoning component of a network security command and control system

Sousa, Gonçalo; Dementis, Georgios

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A LEGAL REASONING COMPONENT OF A NETWORK SECURITY COMMAND AND CONTROL SYSTEM

by

Georgios Dementis and Gonçalo Sousa

March 2010

Thesis Advisor:	James B. Michael
Second Readers:	Thomas C. Wingfield
	John F. Sarkesain

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the 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 Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE A Legal Reasoning Component of a Network Security Command and Control System		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Georgios Dementis and Gonçalo Sousa			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

There are numerous computer-aided tools to enable Computer Network Defense. However, their effectiveness in countering attacks is less than optimal when they are used independently of one another. Research has identified the requirements for an integrated command and control (C2) system that is able to conduct full-spectrum operations in the cyberspace environment. The most notable of that research revolves around the development and experimentation with the prototype system known as Cyber Command, Control and Information Operations System (C3IOS). C3IOS provides for a loose confederation of the cooperating systems with interaction between systems going through C2 interfaces. In this thesis, the authors introduce into C3IOS a means to support the commander's ability to take measured responses to coercive actions in a timely manner, specifically to facilitate the interaction between experts in the law of information conflict and information warriors responding to a cyber attack. The authors' research results in a set of use cases and requirements for the C2 understanding, planning, and deciding activities involved in such a capability, using Schmitt's analysis as an example.

14. SUBJECT TERMS Cyberspace, Cyberspace Defense, Network Defense, Distributed Systems, Command and Control, Battle Management, Information Assurance, Situational Awareness.			**15. NUMBER OF PAGES** 97
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A LEGAL REASONING COMPONENT OF A NETWORK SECURITY COMMAND AND CONTROL SYSTEM

Georgios Dementis
Lieutenant, Greek Navy
B.S., Hellenic Naval Academy, 1995

Gonçalo Sousa
Lieutenant, Portuguese Navy
B.S., Portuguese Naval Academy, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2010

Authors: Georgios Dementis and Gonçalo Sousa

Approved by: Professor James B. Michael
Thesis Advisor

Thomas C. Wingfield
Second Reader

John F. Sarkesain
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

There are numerous computer-aided tools to enable Computer Network Defense. However, their effectiveness in countering attacks is less than optimal when they are used independently of one another. Research has identified the requirements for an integrated command and control (C2) system that is able to conduct full-spectrum operations in the cyberspace environment. The most notable of that research revolves around the development and experimentation with the prototype system known as Cyber Command, Control and Information Operations System (C3IOS). C3IOS provides for a loose confederation of the cooperating systems with interaction between systems going through C2 interfaces. In this thesis, the authors introduce into C3IOS a means to support the commander's ability to take measured responses to coercive actions in a timely manner, specifically to facilitate the interaction between experts in the law of information conflict and information warriors responding to a cyber attack. The authors' research results in a set of use cases and requirements for the C2 understanding, planning, and deciding activities involved in such a capability, using Schmitt's analysis as an example.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AOR	Area of Their Responsibility
BM	Battle Management
CIO	Chief Information Officer
CLT	Consultant Legal Team
CMDR	Commander
CNA	Computer Network Attack
CND	Computer Network Defense
CNO	Computer Network Operations
COA	Course of Action
COIS	Cyber Operations Information System
C3IOS	Cyber Command, Control and Information Operations System
CONOPS	Concept of Operations
CW	Cyber Warfare
CWC	Cyber Warfare Commander
CWC2BM	Cyber Warfare Command and Control Battle Management
C2	Command and Control
C2/BM	Command and Control Battle Management
DDoS	Distributed Denial of Service
DLC	Director of the Legal Cell
DLP DEP	Deputy / Assistant of the Legal Director
IA	Information Assurance (IA)
IA/CND	Information Assurance in Computer Network Defense
IA CONOPS	Information Assurance Concept of Operation
IAOC	Information Assurance Operation Center
IAOPS	Information Assurance Operations
IAVA	Information Assurance Vulnerability Assessment
ICT	Information and Communication Technology
IDS	Intrusion Detection System

IHL	International Humanitarian Law
IR	Intrusion Response
JAG	Judge Advocate General's Corps
KWC	Kinetic Warfare Commander
LA	Legal Advisor
LO	Legal Operator
LOAC	Law of Armed Conflict
MDA	Missile Defense Agency
M&S	Modeling and Simulation
NASA	National Aeronautics and Space Administration
NETOPS	Network Operations
P2P	Peer-to-Peer
PUB/SUB	Publish and Subscriber
ROE	Rules of Engagement
SA	Situational Awareness
TB	Test Bed
UC	Use Case
UN	United Nations
USC	United States Code
VA	Vulnerability Assessment
VLC	Virtual Legal Cell

ACKNOWLEDGMENTS

The authors would like to humbly thank Professor Bret Michael, Dr. Thomas C. Wingfield and Mr. John F. Sarkesain for their patience and support during the research and writing of this thesis as well as their dialog, enthusiasm and passion for the subject of cyberspace defense which was the initial inspiration for embarking on this important journey.

LT Georgios (Yiorgos) Dementis HN would like to express his gratitude to the Hellenic Navy for providing him with the unique opportunity to extend his education at the level of a master degree. I would like to thank my parents, Thodoris and Dimitra, for their love, support and great contribution to what I am. Thank you to my thesis partner and great friend Goncalo, accompanied with all the best wishes for him and his beloved family. Your friendship is definitely one of the greatest gifts I earned here. Finally, I would like to express all my love to my precious family. Thodoris and Christos, you fulfill my life with happiness and the reasons to carry on accessing high. My deepest thanks go to my wife and life companion, Xanthi, for her strength and unconditional support. Thank you my love for your courage, your love and the whole beauty that you provide our family and me. This work is dedicated to you with everlasting love and respect!

LT Goncalo Sousa, first I would like to express my gratitude to the Portuguese Navy for the excellent opportunity to extend my education and professional development. I would like to thank to my family back in Portugal, for their long distance support and understanding. My biggest thanks go to my wife Xana and my daughter Sofia, to whom I dedicate this work, for their love, amazing support, patience and understanding, which were fundamental to my success during this graduate studies, I could never express how much I love you both. At last but not the least, I want to thanks to my friend, Yiorgos Dementis, and his family, for their comradeship, wishing you all the luck and success both professional and personal.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Enterprise-level, distributed command and control (C2) (also known as integrated C2) across administrative domains (i.e., organizational boundaries) for use in cyberspace is a relatively unexplored area of research. C2 paradigms applied in the kinetic world are not necessarily well suited for use in the context of prosecuting engagements in cyberspace in response to cyber attacks. There are many reasons for the mismatch, such as the fact that the tempo of attack is much higher in cyberspace than that of the physical world, precluding the use of serial communication of orders and the use of hierarchical command structures. Concerning cyber attacks, the organization whose cyber assets have been targeted must be able to rapidly understand the nature of the attack through shared knowledge and situational awareness.

> Situational awareness is the process of recognizing a threat at an early stage and taking measures to avoid it. Being observant of one's surroundings and identifying potential threats and dangerous situations is more of an attitude or mindset than it is a hard skill. [1]

The organization must swiftly select courses of action and plans, communicate intent and guidance, task (i.e., synchronize operations, issue plans and orders), and monitor (i.e., assess the following: guidance, compliance with guidance, effects, and achievement of objectives). Given that a single attack can target multiple systems owned or administrated by multiple organizations, these organizations need to coordinate their efforts in advance, to the highest degree possible, through organizing (e.g., coordinating with mission partners, establishing collaborative policies and procedures, integrating capabilities, establishing commander's expectations), planning, developing metrics, and so on.

Research has been done to identify requirements for an integrated C2 model that is able to conduct full-spectrum operations in cyberspace. The problem is that in the context of distributed real-time cyber defense networks,

one misses the legal grounding with respect to the adopted responses. One has to be sure that the means, the timing, and all the ramifications of the response are within the bounds of the law, policy, and rules of engagement. Information warriors used to make decisions based on localized information that they obtained from their Area of Responsibility (AOR), instead of looking at the broader picture of the cyber battle space. Going in this direction, one needs to fully address the problem by looking at the three-dimensional "cube" model introduced by Tom Wingfield and Eineken Tikk. The model depicts "the possible"—representing the technology, "the permissible"—representing the law, and "the preferable"—representing the art of the preferable. Assuming that distributed real-time C2 systems provide solid platforms upon which to conduct cyberspace defense operations, one still needs to accelerate the process of the legal coverage of actions in the ever-changing cyberspace environment.

In this thesis, the authors address the information warrior's challenge of obtaining just-in-time legal advice. They propose the implementation of computer-assisted legal reasoning for integrated C2 in cyber operations. The information warrior needs the right recommendations for action, at the right time, provided by legal experts and others involved in cyber operations, and the ability to obtain timely approval of courses of action by the chain of command. Such a system capability will not dictate the way to conduct cyber warfare, but instead will support the ability of gaining approved legal advice in real or near real-time operations.

An integrated C2 system, with the proposed legal advice capability, can be used either by the military or other actors—including organizations in the private sector—that have a role in defending themselves or others in cyberspace. Any computing resource that connects to the Internet has to have some level of protection, but it may not be economically or otherwise justifiable to protect every computing resource using a full-up dynamic C2 battle management type of system.

There are organizations that have critical infrastructures and systems that need to be protected for the sake of the entity, the organization's customers and stakeholders, or even national security. For example, in the case of the National Aeronautics and Space Administration (NASA) [2], an agency of the United States government, it is responsible for the nation's civilian space program. An attack on one or more of NASA's missions could have an effect on the national security of the United States. NASA is an early adopter of a prototype integrated C2 system called Cyber Command, Control and Information Operations System (C3IOS), formerly known as Cyber Operations Information System (COIS). C3IOS facilitates the defense by NASA of the agency's systems, but C3IOS does not provide the agency with any support on reasoning about the legal ramifications of its defensive posture and any responses it might take in response to attacks on its systems. For example, NASA needs to hand off law enforcement tasks (e.g., collecting evidence to prosecute intruders) to law enforcement agencies.

Regardless of whether C3IOS or a C3IOS-like system is being used in the private or public sector, its roles and hierarchical organization should be based on military principles, such as unity of command. There is still a need to have someone in charge that has the equivalent of a commander's authority and responsibilities—someone who, even if he or she lacks the ability to conduct military operations, still needs situational awareness as well as legal and other support for responsible decision making.

In this thesis, the authors focus on determining what support the defenders of cyber infrastructure and systems need in terms of legal consultation to be able to conduct cyber operations. The thesis reports the results of both a use case and a requirements analysis.

A. BACKGROUND

1. Cyber Command, Control and Information Operations System (C3IOS)

In the open literature, the only reported distributed C2 environment tailored for use in conducting defensive cyber operations is the aforementioned prototype system known as C3IOS. In order to provide cyber-based C2 capabilities, C3IOS relies on distributed computing technologies such as virtual cells, mobile agents, dynamic reconfiguration, and IP address hopping. C3IOS also provides for proactive and anticipatory collaboration.

The services orientation of C3IOS makes it possible to enable collaboration among operators, technical experts, and other decision makers as needed. The dynamic virtual cell is one of the defining characteristics of C3IOS. The dynamic virtual cell is a virtual community where people can join or leave before, during, or after a cyber incident. In C3IOS, the C2 system consists of two sets of virtual cells: core and dynamic. The seven core cells consist of full-time members who perform rapid-reaction, engineering operations, system administration, and other daily duties to carry out cyber defense (e.g., Kinetic Warfare Commander, Cyber Commander, network operations, vulnerability assessment, intrusion detection, intrusion response, and test bed [engineering]) [3]. Those roles and activities are not persistent and can be adjusted to meet the organization's needs. The dynamic cells can be configured to contribute to the progress of a specific task and decommissioned thereafter.

C3IOS does not dictate how to defend systems; instead, it provides battle management (BM) and C2 capabilities. The current version of C3IOS does not provide users with support for reasoning about the law as it pertains to conducting computer network operations.

2. Schmitt's Analysis

A cyber incident can have various forms that can be generally categorized into planned malicious cyber actions, immature efforts to put a false color on national/private services, and the uncontrolled spread of malicious rogue code via worms and viruses. The malevolent actor tries to harm the targeted system or infrastructure. Regardless of whether the protection of systems and infrastructure is the responsibility of the public sector, private sector or both, the defense of the system or infrastructure must be conducted within the bounds of the law, to include international law when attacks cross national borders.

> Applying a "one-size-fits-all" response, such as always terminating all interaction with the rogue agent or always responding in kind can be an ineffective or worse, illegal, response. For instance, terminating interaction with a rogue actor may prevent the collection of evidence for criminal prosecution, counter-targeting for military response, or collection for a counterintelligence operation. By responding in kind, or conducting some form of cyber vigilantism as described in [Jayaswal 2002], the owner or the owner's agent may violate domestic laws, or if the attack is deemed to be a "use of force," may contravene the customary rules of war (accepted as authoritative law by the United States and punishable under 18 U.S.C. §1097). [4]

The authors' work is under the framework presented by International Humanitarian Law (IHL), which is also referred as the Law of Armed Conflict (LOAC). IHL "defines the conduct and responsibilities of belligerent nations, neutral nations and individuals engaged in warfare, in relation to each other and to *protected persons*, usually meaning civilians." [5] The law has two parts to include the law of conflict management (*jus ad bellum*) and the law of war (jus in bello).

Under the imaginary framework created by the ethical behaviors and the rules of law presented by the LOAC, Chapter II of this thesis introduces Schmitt's analysis as an example of interpreting the existed law in the context of conflicts in cyberspace. Schmitt's analysis can be applied to distinguish operations in accordance with the spectrum of their induced consequences, and postulate

either the use of force or soft countermeasures [6]. The contribution of this method of analysis is not to propose the actions that might need to be taken against a cyber incident, but to indicate whether the incident at hand will rise to the threshold of an armed conflict. It provides a practical framework to analyze the effect of key factors on the legal nature of an incident to unravel the real dimension of the imposed consequences [7].

Schmitt's analysis answers the question of whether an attack has risen to the level of use of force as defined in the Charter of the United Nations and Statute of the International Court of Justice, taking into consideration qualitative and quantitative information about the methods and the consequences of the attack. In order to evaluate the methods and the consequences of an attack, Schmitt's analysis looks to seven criteria: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility that characterize the attributes of an armed attack.

It is not the authors' intention to automate Schmitt's analysis, but rather to provide a collaborative environment in which to bring people involved in cyber defense in contact with legal experts to facilitate informed decision making about defensive posture or responses to cyber attacks. Schmitt's analysis is used here as a case study.

B. OBJECTIVE: A PROPOSAL FOR A NEW DYNAMIC VIRTUAL LEGAL CELL IN A DISTRIBUTED REAL-TIME CYBERSPACE DEFENSE SYSTEM

In order to take into consideration the legal ramifications of actions that might be taken in response to a cyber attack, the authors propose the creation of a dynamic Virtual Legal Cell for C3IOS. The proposed Virtual Legal Cell, presented in Chapter III, needs to be added to C3IOS to support the commander's ability to take measured responses to coercive actions. In order to take into account the qualitative and quantitative aspects of a cyber incident, the authors investigated how Schmitt's analysis could be made part of this cell.

The thesis focuses on the C2 understanding, planning, and deciding activities involved in applying Schmitt's analysis within this new virtual cell for C3IOS. The authors present a set of use cases and requirements for these activities.

C. CONCLUSION

A real-time distributed cyber defense network is essential to address coordination issues, support rapid information gathering and finally, maintain real or near real-time responses. Since the legal reasoning aspect of cyber operations plays an integral part in shaping responses to cyber incidents, the authors propose a way to get legal experts engaged in a timely manner in a cyber operation and provide these experts situational awareness. On the other hand, given that the acquisition of the legal piece/grounding can be time consuming, the lumped lag (i.e., sum of the delays) in making decisions can slow the whole process dramatically and preclude timely responses. The authors propose the creation of a dynamic Virtual Legal Cell for C3IOS, which will be able to be created on demand to support the decision-making process.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CYBER COMMAND, CONTROL AND INFORMATION OPERATIONS SYSTEM (C3IOS)

The defense community relies heavily on interconnected information systems. These systems cannot rely solely on traditional defense-in-depth strategies to address information security concerns. In addition, systems for controlling the remote management of firewalls, intrusion detection systems (IDS), and other network components and subsystems cannot always provide appropriate responses to attacks or even provide information to decision makers about impending attacks in a timely manner.

One can model modern defense systems as systems of systems, in which the collective behavior provides some added benefit that none of the individual systems acting autonomously can provide. In doing so, one must consider the emergent behavior (both desired and undesired). The constituent systems may be governed by different entities. Having system-of-systems-wide C2 capabilities is needed to ensure that defenders can obtain situational awareness of the cyberspace the system of systems occupies.

The U.S. Missile Defense Agency (MDA) introduced an operational model for a virtual organizational structure called the Information Assurance Operations Center (IAOC) accompanied by a Concept of Operations (CONOPS) and a summary of the system model infrastructure [3]. Additions were made to the IAOC to provide for a full-spectrum Cyber Warfare Command and Control Battle Management system (CWC2 BM), and the working prototype, as mentioned earlier, was named C3IOS.

NASA explored the use of C3IOS in maintaining cyber warfare situational awareness (SA) of NASA computer networks, supporting collaboration among members of the various operational communities within the IAOCs, and enabling collaboration among other desired members of differential, pre-existing or not, supportive communities [8]. The IAOC implemented a peer processing architecture system for C2. In this architecture, local data storage is available on

all nodes, messaging is accomplished based on a publish/subscribe pattern, and identical application suites are run on all nodes. The IAOC employs a virtual organization in a distributed network virtual organization to ensure the partial or full exchange of information among its participants to network participants in order to defend enterprise network computing assets against cyber attacks.

The original intent of the creators of C3IOS was to provide the cyber defense community a full-spectrum cyber warfare C2 system with the aim of establishing effective cyber defense strategies, while at the same time improving both SA and addressing organizational issues. In order to address typical delays with traditional client-server architecture, C3IOS employs a publish/subscribe messaging pattern as well as a virtual shared data space that minimizes data queries generating and presenting situational awareness. Contributing to delays and generating SA include request-reply messaging patterns, as well as querying, tailoring and presenting data to convey SA to a user. Peer-processing architecture (in particular, the publish/subscribe pattern and local data storage), is what contributes to the ability to generate rapid SA. The architectural characteristics employed by C3IOS permit a real-time SA for on-demand provisioning of services and facilitate the rapid development of COAs. The ideas of deliberate planning (i.e., having a plan given some scenario) and crisis planning are only partially appropriate in cyber warfare. The depth and breadth of unknowns in cyber space dictate a more dynamic planning model that in part is stochastically based. On the other hand, C3IOS uses dynamic planning based on a stochastic model. Contrary to kinetic warfare, in cyber warfare it is difficult to predict or know a priori the behavior, attack vector, or signature of interest. COAs are often deployed based on chance. On the kinetic and cyber battlefields, commanders' make decisions under uncertainty with less than 100 percent SA. On average, in kinetic warfare one may have 80% knowledge of the battle space, while in cyber warfare one probably has 20% knowledge. In addition, in distributed systems, one only has partial knowledge of the state of the systems; that is, one does not have real-time global knowledge of the state of the

distributed system [9]. Attacks like distributed denial of service (DDoS), in which the execution path is known, can be captured in via planning and this knowledge can affect the COA. However, there are other types of attacks that are unknown before they are launched against a target.

As stated in the C3IOS user manual, the purpose of the system is to provide rapid coordination response and C2 of “defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction [10],” also called Computer Network Defense (CND). The dynamic CND provided by C3IOS has the capability to manage the various security defense tools/information to support rapid C2 decision making, response and command mechanisms to sustain a broader set of capabilities to maintain SA. C3IOS generates a widespread real-time operating picture of the status of the network presented on the enterprise network display and current attacks or cyber operations in different displays (e.g. cyber order of battle display, attack status display).

In addition, C3IOS provides a common and trusted virtual environment in which subject matter experts located in different physical locations from can cooperate to coordinate their actions across organizational and role-related lines [8]. At this time, it is only partially trusted, but the intent is to provide end-to-end security.

The CND CONOPS is based on a virtual cell organizational model. The requirement that led to the adoption of the virtual cell approach, via the use of physical cells, was the need for a high level of flexibility and rapid response to a cyber incident. In traditional kinetic warfare, subordinate decisions of C2 systems are controlled and must be approved by the appropriate person or people in the chain of command in a serial manner before being executed. In the case of cyber defense, this type of time-consuming serial communication can prove to be inadequate in handling cyber incidents, as such incidents can unfold within seconds to a minute (e.g., zero-day attacks) and the battle can be over in as little as a few minutes.

For critical infrastructure and systems, Information Assurance Vulnerability Assessments (IAVA) [11] must be established in real time or near real time. The scope is to mitigate potential vulnerabilities to avoid situations of one-sided battles, in which the attacker completes or causes operations even before the target's defense mechanism can detect the attack or respond. However, the reason IAVAs cannot be pre-established is due to the way the process is implemented. When an attack or vulnerability is identified, everybody is notified and is given a certain amount of time to patch it. However, in practice this is difficult to do. During a zero-day attack, there is no way to identify which type of patch is going to be needed. When the attack appears with no warning, there is no way to respond in real time; it is this sort of out-of-band process that needs to be in-band. In this sense, the virtual cell model is more appealing than the physical cell model because it provides users of C3IOS with the flexibility to dynamically join virtual cells in order to participate close to the field of action. The virtual cells are more advantageous than physical cells for this type of warfare as they provide speed and flexibility across network boundaries and organizations, which is difficult to do in traditional C2 models or organizations.

The system relies on virtual organization operational architecture and a peer-processing system architecture (i.e., all nodes on the network have the same application suites). This peer-processing system architecture compliments the operational architecture by employing peer-to-peer virtual cells. Furthermore, each of the members of a cell can be in more than one virtual cell concurrently, thereby integrating and coordinating multiple tasks that have dependencies. In C3IOS, the cell model is based on membership relationships versus the traditional C2 reports-to relationship. By employing this cell membership model for C2, one can maintain the command structure while simultaneously leveraging the power of peer-to-peer operations. This many-to-many relationship generates the network relations and allows the chain-of-command relationship to be embedded in the organizational structure for cyber warfare [11], thus retaining the ability to operate efficiently under the hierarchical warfare command structure

for the cases where cyber warfare must be part of an integrated kinetic warfare C2 system. Finally, the dynamic creation, repositioning, and decommissioning of virtual cells increase the resistance to attacks and fault tolerance. Figure 1 illustrates the basic differences between the virtual P2P operational architecture way of organization and the strictly hierarchical kinetic one presented by physical cells.

In addition, the virtual organization created with virtual cells can facilitate tactics like deception and maneuver [11] to provide the defender with a more flexible and dynamic defense against attack. When cleverly using pub/sub and the power of virtual cell integration in this architecture, one can rapidly disseminate SA and use cell integration to coordinate and collaborate, thus providing for an anticipatory posture rather than static reactionary ways to counter a cyber attack. C3IOS architecture can be anticipatory because if one node is subjected to an attack, the agent or sensor that detects the attack can automatically start publishing information about the attack to all of its peers. An attack on a machine in California instrumented with C3IOS can publish data about the attack to another node on the East Coast before that other node is subjected to the same attack, thus providing the opportunity for the enterprise to develop or deploy defenses against the attack before it arrives.

Applied models or approaches, among others, are dynamic reconfigurations of systems, honeynets, mobile agent patrols, secure publish/subscribe communication protocols, movements of states, and virtualization for deception purposes. These advanced techniques provide for a more dynamic defense posture and operational capability. For example, if an attack happens or there is some other fault on a node (e.g., cyber), with a peer processing architecture supported by publish/subscribe, it is possible to move (via publication mechanism) the last known valid state without losing any continuity. This assumes another node is running the same application suite in a

non-engaging way. From the perspective of fault tolerance, the use of publish/subscribe provides for moving the last state to another copy of the application running in a different node.

The use of deception tactics, such as IP address hopping, attempts to confuse potential attackers and present a changing logical structure. Similarly, honeypots can be applied to detect, repel or neutralize attempts of unauthorized access [12], or just to get attackers to waste time trying to attack the honeypot rather than a target of value [13]. In C3IOS, honeynets are configured in such a way that all activities are monitored, recorded and discretely regulated [14].

A maneuvering tactic can be implemented by employing the dynamic reconfiguration of the system or by reallocating virtual cells, thus making it difficult for a potential attacker to attack the cells. Another important feature of the system is the mobile agent. A mobile agent is a process that is able to move its state from one environment to the other, and to move between computers anytime during its execution.

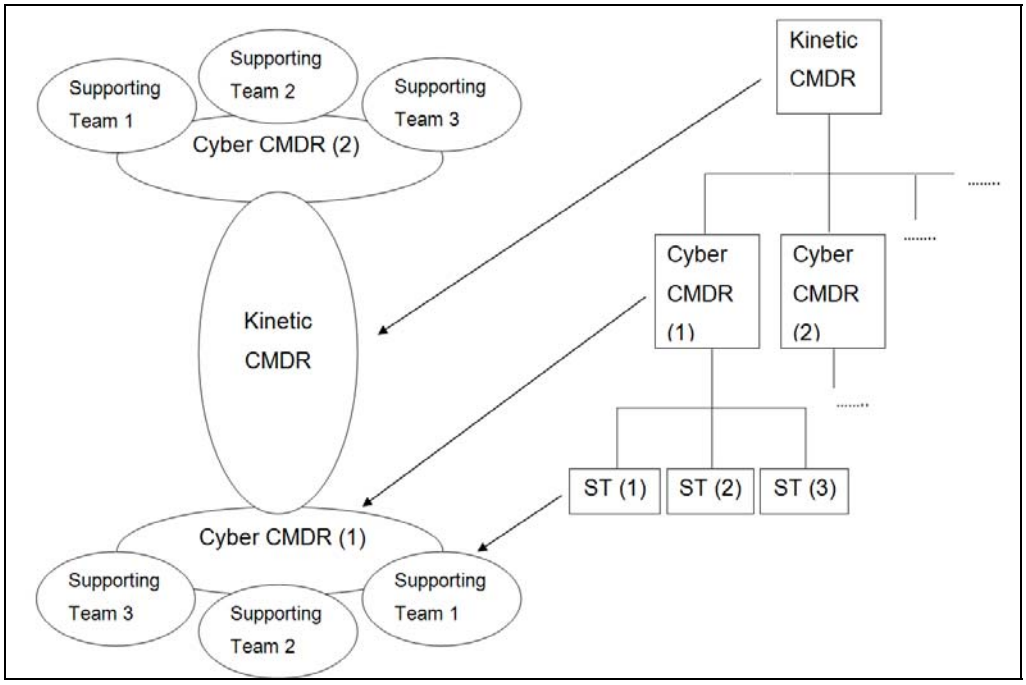

Figure 1. Virtual and Physical Ways of the Organization (From [8]).

This special attribute makes them in general a powerful tool for implementing distributed applications in a network [15]. In particular, they can be used for mobile intrusion detection sensors. When they discover an anomaly (vulnerability, a hostile signature or an attack), they can publish this information to other agents as well as cells, and thus provide an anticipatory intrusion detection model. They can also be implemented with broadcast or multicast techniques. Since the subscriber does not need to know where the publisher is located and conversely the publisher does not need to know where the subscriber is, they are highly autonomous and loosely coupled [15]. This has many advantages in any distributed computing application (e.g., scalability across large enterprises).

When the aforementioned dynamic capabilities are employed through the execution of C3IOS, a highly dynamic cyber C2 capability is achieved. This capability extends beyond the benefits of traditional information assurance controls and defense-in-depth strategies. With the C3IOS architecture, IA controls are integrated to create a more synergistic cyber defense posture and used to rapidly generate SA. Furthermore, the use of the virtual organization's cells, virtual shared data space, and pub/sub messaging provide for a system and operations architecture that facilitates and provides the capability to conduct real-time full-spectrum cyber operations across network and organizational boundaries.

Note, that cyber warfare is a technical activity in terms of the prosecution of engagements. The people that fight cyber wars need to have some level of technical competency, although efforts have been made to minimize the needed level of competency, especially the efforts to make the low-level details of how defensive and offensive weapons and sensors work as transparent as possible to the information warriors [16].

C3IOS has a wide variety of displays available to the user for such things as situational awareness, cyber order of battle, attack status, task management, drill-down of simulated attacks, and vulnerability status. Some of these ideas, like

cyber order of battle, are evolving. In addition, C3IOS supports COA formulation, execution, and simulations. Furthermore, it employs cyber engineering cells to integrate cyber operational, training, rapid cyber weapon development and testing capabilities. Figure 2 illustrates the existing CND virtual structure of NASA, which is based on the membership relation. Although cyber warfare is not NASA's primary mission, cyber warfare capabilities are integral to ensure mission success and national security. The shaded areas indicate members belonging to both communities [8].

C3IOS technology can be used by both civilian and military organizations. It is generally accepted that cyber defense is not a purely military activity. For example, Presidential Security Directive/NSC-63 (May 22, 1998) discusses the need to establish a public-private partnership to protect the critical infrastructure of the United States. C3IOS can be deployed in any critical infrastructure (e.g., the power grid, national air traffic control system); civilians are responsible for the operation of the critical infrastructure. C3IOS permits the civilian defenders to leverage the same operational model and a CONOPS consistent with the military cyber C2 architectures. Names, roles and responsibilities might be different. The NASA C3IOS manual illustrates the U.S. DoD's role and NASA's command structure for cyber defense. NASA's Chief Information Officer (CIO) is equivalent to the DoD's Cyber Commander or Kinetic Warfare Commander. The other communities in the example are the Cyber Warfare (CW) and Goddard CW (one of the many centers within NASA) communities, the Intrusion Detection (ID) community, the Intrusion Response (IR) community, the Vulnerability Assessment (VA) community, the Network Operations (NETOPS) community, and the Testbed community. Every one of the core community teams consists of core members who have joint duty stations twenty-four hours a day, seven days a week.

The CW community maintains the higher level of command in the cyber warfare command structure and is responsible for choosing strategies and tactics to defend the center's network [8]. Note that national policy and doctrine define

how strategies and rules of engagement (ROE) will be defined. It establishes/updates the status of the ROE and authorizes any action/counter measure that needs to be taken. Each regional CW is supported by the rest of the aforementioned communities (ID, VA, IR), which represent subordinate communities in that each one of them holds ad hoc tasks. The C3IOS architecture can adapt to any organizational command structure, both syntactically and semantically, and this is why it was adopted by NASA, even though C3IOS was originally designed for use by the DoD.

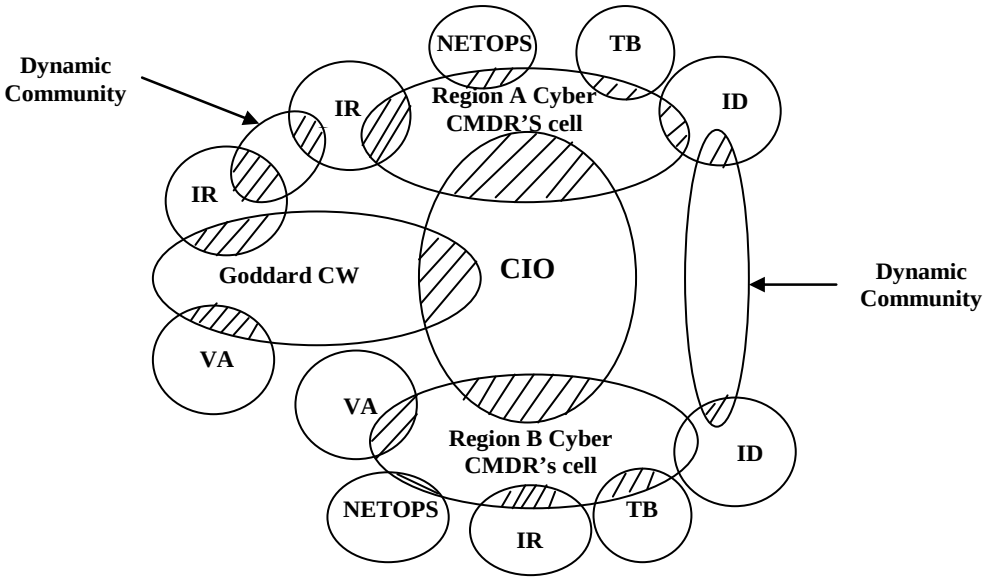

Figure 2. Virtual Community Structure (From [8]).

The ID community controls and monitors all of the available sensors and mobile agents in order to acquire timely host and network intrusion incident information [8]. The particular community is also responsible for conducting forensics on compromised or suspect center systems in the NASA example. Those types of data should be securely stored in an appropriate format and be accessible by the authorized cells. This category of sensors includes, among others, intrusion detection scanners, host-based IDS, firewalls, and mobile agents on duty to patrol the C2 system or dispatched with an assigned duty to achieve (e.g., to reconfigure sensors) [11]. As the information is acquired, it is

passed to the IR community. Again, in this section each cell can have varying responsibilities based on commander's intent, doctrine, policy, ROE and other factors related to the mission.

The IR community is responsible for proposing and executing—after the authorization of the CW commander—the actions needed to be employed against the attackers [8]. In order to respond in the most appropriate, lawful and efficient way, the commander need to obtain updates regarding the current status of the ROE in force and the availability of hardware/software offensive means. Besides the main task to execute a response, the IR community also provides recommendations with respect to the adopted COA and executes damage assessments to estimate the level of success of the engagement [11].

The Network Operations (NETOPS) community ensures operational readiness of the available computer and network assets to support the center mission and encounters vulnerabilities and network-design weaknesses discovered by the VA and ID communities [8]. The VA community works closely with NETOPS and engineering to mitigate vulnerabilities. NETOPS is also responsible for an imminent and efficient recovery, which includes actions such as restoring backed up data or reconstituting servers/networks.

The Testbed (TB) community assists in communications and collaboration with the contractor engineers and other organizations working with the IAOC. All personnel, regardless of the different levels of expertise, require cyber operations training [8]. In the IAOC, there exist two different states of operation: the normal and the emergency state. In the first state, the communication and collaboration relates to operational testing of the IAOC and the new functionality of C3IOS or products integrated into C3IOS. In the emergency state, the communication and collaboration relates to emergency support to the IAOC, including using the testbed as an emergency backup to the IAOC, as a large-scale honeypot (e.g., as a honeynet), for rapid attack response code generation; and modeling and simulation (M&S) activities in support of an IR operation [8].

Finally, as Figure 2 illustrates, in addition to the core communities there exist dynamic ones that can be created for a specific task or operation and decommissioned after the task or operation is finished [8]. Any cell commander can authorize subordinate communities within its community or peer-level virtual communities at the tactical level. Anytime a cell commander authorizes the creation of a virtual cell, he/she is responsible to authorize membership, monitor the cell, and authorize decommissioning when necessary.

Prior to 2004, the work on C3IOS included the completion of the IAOC CONOPS, the C3IOS Users Manual, the IA/CND CONOPS, the CyberC2 Users Manual, and the Prototype CyberC2 tool-set (Version 3 for Linux and Windows delivered April 5, 2004) [17]. During 2004, work continued with the establishment of a cyber C2 testbed operation at the Institute of Defense Analysis and Houston sites, along with work on a secure high-performance publish-and-subscribe messaging infrastructure. The IAOC is now considered an out-of-date concept.

The thrust of the work on C3IOS at present is to make it possible to deploy C3IOS across any enterprise, or even the national communications infrastructure and the global information grid, i.e.,

> globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. [18]

C3IOS, can be used to conduct and mange full spectrum cyber warfare, which was from the beginning what the inventors always intended for this system.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SCHMITT'S ANALYSIS

After the September 11, 2001, attacks, the whole world started to pay added attention to both kinetic- and cyber-based terrorist threats to national and international security.

> Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not. [6]

Examples of the types of motivation for conducting an act of terrorism are financial, political, military, religious, and ideological. Attacks in cyberspace can have the same effect as kinetic attacks, such as a terrorist, member of an organized crime syndicate, or nation-state-sponsored information warrior sending malicious commands to a computer system that controls some energy source. An example of this would be the control system for automated passenger trains. The sending of malicious commands to its computer system could produce a mishap (e.g., two trains entering the same segment of track and colliding), resulting in death, injury, and property damage.

Society is becoming ever more reliant on computer systems. Examples include electronic banking, electronic government, telemedicine, and smart power grids. All these systems are vulnerable to attack.

Cyber conflicts can be analyzed in light of two areas of international law: *jus ad bellum*, also known as the law of conflict management, and *jus in bello*, the law of war. *Jus ad bellum* is the law governing the resort to the use of force—

whether force is permissible or not, and *jus in bello* is the law that governs activities once *jus ad bellum* has determined that force may be used. The United Nations Charter clarifies it with the relevant articles mentioned below.

Article 2(4):

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. [19]

Article 39:

> The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security. [20]

Article 51:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security. [20]

In a case of an attack, according to the above articles, the following four-level hierarchy can be considered:

1. Below Article 39, international peace and security.
2. Between Article 39 and Article 2(4), comprised of threats to international peace and security.
3. Between Article 2(4) and Article 51, made up of uses of force—unlawful, but not permitting an armed response.
4. Above Article 51, an armed attack—actions that permit (but do not require) an armed response because the inherent right of self-defense has been activated.

Do the concepts of use of force or an armed attack apply to operations in cyberspace? The answer is not always clear, because cyber attacks can have minor consequences, but devastating ones as well. Professor Michael Schmitt created criteria for evaluating the consequences of cyber attacks. Professor Thomas Wingfield extended Schmitt's analytical technique by providing a means for quantifying the qualitative measures of consequences. The seven characteristics are listed below:

- "Severity: Armed attacks threaten physical injury or destruction of property to a much greater degree than other forms of coercion. Physical well-being usually occupies the apex of the human hierarchy of need." [21] This characteristic refers to people killed or wounded and property damaged.
- "Immediacy: The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case." [21] Immediacy is the time it takes for the consequences of an operation to take effect.
- "Directness: The consequences of armed coercion are more directly tied to the actus reus than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty." [21 This characteristic refers to the relationship between an operation and its effects.
- "Invasiveness: In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability." [21] This characteristic Involves crossing borders.
- "Measurability: While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein,

less suspect in the case of armed force." [21] Measurability is the measure of the effect of the operation, either in number of victims or the value of the property damage.

- "Presumptive Legitimacy: In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory." [21]
- "Responsibility: refers to the degree to which the consequence of an action can be attributed to a state as opposed to other actors. The premise is that armed coercion is within the exclusive province of states and is more susceptible to being charged to states, whereas non-state actors are capable of engaging in such soft activity as propaganda and boycotts." [6] This characteristic refers to the degree that the consequence of an action can be attributed to a party.

By contrast, most other forms of coercion—again in the domestic and international sphere—are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).

The law of war is defined by the United States Department of Defense as

> That part of international law that regulates the conduct of armed hostilities. It is often called the law of armed conflict. The law of war encompasses all international law for the conduct of hostilities binding on the United States or its individual citizens, including treaties and international agreements to which the United States is a party, and applicable customary international law. [22]

The above law is précis applying seven principles:

- "Distinction of combatants and noncombatants, only members of a nation's regular armed forces may use force, and they must distinguish themselves and not hide behind civilians or civilian property.
- Military necessity, targets of attack should make a direct contribution to the war effort or produce a military advantage.
- Proportionality, when attacking a lawful military target, collateral damage to noncombatants and civilian property should be proportionate to military advantage likely to be achieved.

- Indiscriminate weapons, weapons that cannot be directed with any precision, such as bacteriological weapons, should be avoided.
- Superfluous injury, weapons that cause catastrophic and untreatable injuries should not be used.
- Perfidy, protected symbols should not be used to immunize military targets from attack, nor should one feign surrender or issue false reports of cease fires.
- Neutrality, nations are entitled to immunity from attack if they do not assist either side; otherwise, they become legitimate targets." [6]

Regarding combatants and noncombatants, military necessity and proportionality guarantees that wars should only be carried out by military forces, and the targets should be only military in character as well. The prohibitions against indiscriminate weapons and superfluous injury assure that no excessive means are used in conducting an attack, while perfidy and neutrality pledge immunity for either using protected symbols or not assisting the involved parts in the conflict.

Moreover, cyber conflicts can be divided in three different categories:

- "Cyber warfare at the state level when conducted in the interest of national security." [6]
- "Non-state actors whose cyber attacks are politically or socially motivated," [6] and
- "Cyber defense, particularly what is called hack back, strike back, or active response." [6]

The point is not to create responses for the above categories but instead present a framework that will determine if a specific cyber attack warrants the use of force and if it follows the law of information conflict.

Estonia is considered one of the most developed countries in terms of its use of information technology, from being the first to use online voting to having almost all government agencies virtually connected. Estonia holds the lead in online banking, with about 95% of its banking operations being processed this way. Students in Estonia's schools can get their exams results by Short Message Service (SMS) and parking fees can be paid via mobile phone interface [23].

The attacks on Estonia in 2007 had an impact on the security of the nation [23]. The point is that not only the developing of the attack, but that all the dependency in computer-assisted systems creates higher vulnerabilities that can lead to catastrophic disasters.

Moreover, the United Nations (UN) Charter takes a qualitative instead of a quantitative approach. The UN Charter framework was meant to diminish military actions, mainly military oppression between countries, even if that implied an increase in the use of economic or diplomatic coercion. The problem with this framework is that not all types of violence fit within the UN Charter parameters. Broad forms of violence (e.g., terrorism) are left out of the spectrum of what the UN Charter relates to, yet these forms of violence are also capable of at least the same mass destruction and deaths as the ones in the spectrum of the UN Charter.

Laws (implemented either by force or by sanction), social norms, markets, and architectures regulate cyberspace. How one can address and measure cyber terrorism goes towards answering the question of “did the attack rise to the level of use of force?”

Using common sense is not sufficient to answer this question. This is where Schmitt’s analysis has an important role to play by attributing a degree to each of the seven criteria and addressing the grey areas of the law by complementing them with a framework that will help to protect first of all lives, and then public and private property. This will allow cyber-intelligence measures to be within the legal bounds. In addition, this analysis will highlight the aforementioned grey areas, which will provide a way to address them in all the important aspects against cyber terrorism.

Using Professor Schmitt’s words, “…as the nature of a hostile act becomes less determinative of its consequences, current notions of ‘lawful’ coercive behavior by states, and the appropriate responses thereto, are likely to evolve accordingly.” [21]

Consider attacks on transportation systems, such as passenger trains. Terrorists conducted kinetic attacks against train systems in Madrid in 2004 [24] and London in 2005 [25]. In 1995, members of the Aum Shinri-kyo cult carried out a sarin gas attack on the subway in Tokyo [26]. What if these attacks had been conducted using cyber means?

Michael, Wingfield, and Wijesekera used Schmitt's analysis on a hypothetical attack of a subway system [7]. They considered two scenarios: one involving a kinetic attack and the other a cyber attack. For the kinetic attack involving the use of sarin gas during rush hour, the severity was rated as an 8 (on a scale from 0 to 10, with 10 as the highest level of severity), because of the number of people injured, the number of deaths, the amount of property damage, and the loss of intangible property. Immediacy was given an 8 because the attack took a matter of minutes, yet the effects could be long term (e.g., decontaminating, psychological effect on ridership). Directness was rated as 8 because the effect could be determined form the cause, as the possible cause was the trains were attacked by terrorists. Invasiveness was given a 9, since the terrorists probably came from other countries. Measurability was an 8, as the number of lives taken could be counted and the monetary value of the lost property could be estimated. Presumptive legitimacy was an 8, because no nation or group has the right to carry out such an attack. Responsibility was a 5, because no one took responsibility for the attack. Therefore, the total of all the ratings was 54 with an average of 7.7 per rating.

For the cyber attack scenario involving the hacking of the subway's automatic train protection (ATP) system, the severity was 8 due to the collision of several trains resulting in multiple deaths, injuries and loss of property like in the kinetic attack. Immediacy was a 9, as even if the crashes occurred in a short amount of time with immediate effects, consequences (e.g., removing vulnerabilities in the software and restoring the confidence of passengers) took a lot of time to clear. Directness was 9, because one act had one effect. Invasiveness in this case was lower than for the kinetic attack because the attack

could be initiated from anywhere in the world. Measurability was a 9, because the effect of the attack could be measured but other effects could not be measured (e.g., loss of public confidence). Presumptive legitimacy was a 5 for the same reasons given for the kinetic attack scenario. Responsibility was a 5 because even if none of the modifications on the system software was understood when executed, according to the “repsia loquitur,” (the common law of negligence states that the elements of duty of care and breach can be sometimes inferred from the very nature of the accident even without direct evidence of how any defendant behaved [27]), the injuries of the passengers were a natural resort of a careless action. Therefore, the total of all the ratings was 50 with an average rating of 7.1. The important thing to note from the two attack scenarios is that the cyber attack had a similar overall ranking to that of the kinetic attack.

In this thesis, the authors investigate how Schmitt’s analysis can be integrated into C3IOS, but they recognize that other types of legal analysis would also need to be made available in C3IOS.

IV. THE PROPOSED VIRTUAL DYNAMIC LEGAL CELL

One of the challenges in cyberspace is to define and detect a hostile act or the use of force. Another major challenge is to respond to cyber attacks in a timely and lawful manner. In this chapter, the authors discuss the need for C3IOS functionality to be enlarged to support reasoning about the lawfulness of COA in response to cyber attacks. The authors refer to the part of C3IOS that will provide the user with this capability as the Virtual Legal Cell (VLC). The aim is to provide users of C3IOS with the ability to obtain an early-as-possible qualitative and quantitative grounding for the appropriate response to a cyber incident, taking in to consideration the legal perspective of the action. There are two aspects of this cell: a dynamic aspect and a virtual one. By dynamic aspect, the authors mean that the cell can be allocated and deallocated as needed. The VLC is the specific virtual space in which experts in the law of information operations can interact with the other users of C3IOS.

The legal cell will be responsible for conducting investigations and forensics analyses to enlighten areas of uncertainty or disagreement in multiple legal analyses, and will recommend actions by proposing the most accurate response plan (RP) concerning the adopted level of use of force in accordance with national/international law and the rules of engagement (ROE) in force. In order to be able to accomplish its duty, the center legal advisor (LA) community maintains a repository of all laws and policies and information about the attack. In order to address the growing threat of cyber intrusions, an academically comprehensive and operationally complete legal framework is needed based on multiple sources of information [4] (i.e., international, constitutional, legislative, executive, and judiciary). The VLC needs two interconnected decision trees: one for computers to execute autonomously at high-speed hardwires for independent implementation of clearly distinguishable, objectively verifiable criteria; and the second requiring human decision making and lower speed, requiring pre-selected sources available to support lawyers in the “grey area” judgments [4].

For this reason, actions are also synchronized with the center NETOPS community to ensure that the VLC always maintains capable hardware and software resources to carry out its operations, as a form of on-demand provisioning.

The Kinetic Warfare Commander (KWC) and the subordinated Cyber Warfare Commander (CWC), or their equivalent in the non-combatant case, can authorize the instantiation of a new VLC.

C3IOS does not impose an organizational structure. In the example shown in Figure 3, there exist two VLCs that were created for two different decision-making situations. VLC D is in a joint community with the ID cells of two different regions, while VLC E was created by the KWC or the CWC to support the decision making taking place in region A.

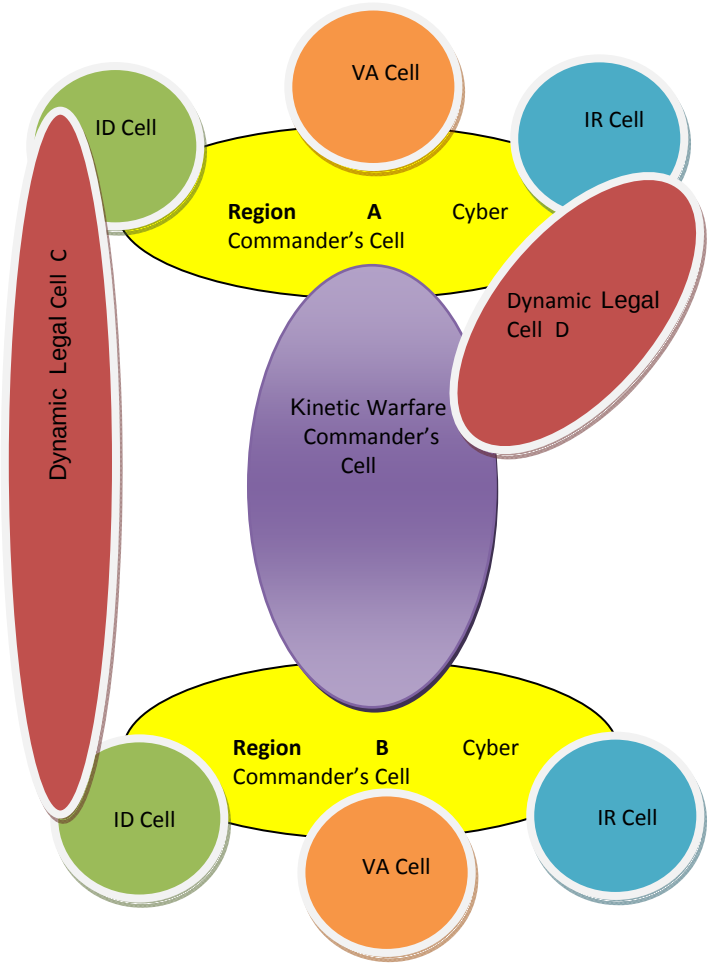

Figure 3. Organizational Model.

A simple vision for the roles of the members of the legal community can be as follows.

Director of the Legal Cell (DLC):

- Views any screen of the community
- Assigns new tasks to the members of the community
- Authorizes the final legal report and provides the final legal advice to the commander who initially authorizes the creation of the cell.

Deputy/Assistant of the Legal Director (DLD DEP):

Assists the DLC and assumes the duties of the director when he/she is absent.

Consultant Legal Team (CLT):

- Group of lawyers and legal scholars (team of three) qualified and specializing in the law of armed conflict in cyberspace
- View ID reports, resources, and statistics
- Execute Schmitt's analysis and forensic analysis
- Generate legal reports and present the results of their assessments to the director of the cell.

Legal Operator (LO):

- Views any screen of the community
- Receives all data and information from other communities (i.e., CWC, ID, VA) with respect to the current cyber incident
- Exchanges messages with the community members and members of other cells where the communication is authorized (i.e., the ID community etc.)
- Verifies information with NETOPS to accomplish hardware and software availability.

From the time that the LA community is formulated, it continuously monitors reports from the Intrusion Detection (ID) cell and the other regional communities. The first aim is to collect all the available information regarding the cyber incident. Second, the legal community needs to check and analyze the sources of evidence for the unauthorized events. The legal experts review the incident by applying techniques such as Schmitt's analysis.

The purpose for conducting the analyses is to minimize the level of uncertainty associated with the incident, thus allowing for an informed decision about which technically feasible COA is best in terms of being congruent with law, policy, and ROE.

As part of the development of the legal cell, the authors focused on the requirements for the C2 understanding, planning, and deciding activities of the VLC.

Before determining how the VLC will be implemented, it is important to identify the qualitative nature and quantitative intensity of the threat. There are two major types of cyber attackers: state actors (those who act on behalf of a

government of a country) and non-state actors (e.g., recreational hackers, terrorists, organized criminals). State actors are easier to identify, and by attributing their actions to specific governments, one can address three thresholds in international law (Articles 39, 2(4), and 51 of the United Nations Charter) which divide the spectrum of violence into the following four zones:

Below Article 39: This condition is known as "international peace and security," and while it does include various forms of political, economic, and diplomatic coercion, it is the preferred zone of international law because of the low levels of direct violence it employs.

Between Articles 39 and 2(4): Here are "threats to international peace and security," as determined by vote of the UN Security Council. These are usually nonmilitary threats with the potential to cause widespread suffering or provoke military action if unaddressed.

Between Articles 2(4) and 51: A "use of force" is qualitatively military, but below the threshold that permits an armed response. The intent of Article 2(4) is to identify unlawful military actions, while at the same time creating a requirement on the part of the defending nation to limit its response and avoid conflict escalation.

Above Article 51: An "armed attack" has taken place whose quantum of violence is sufficient to activate the inherent right of self-defense and permit an immediate, unilateral use of military force in response.

The determination of which zone applies is the heart of *jus ad bellum*, which is the question of whether or not force may be applied. If that determination is affirmative, then *jus in bello* determines how that force may be applied, namely the limits of violence in a wartime setting.

Although there is a clear academic distinction between state and non-state actors, real-world examples are more complicated. There is a sliding scale of certainty (given the opaqueness and anonymous nature on the Internet), and a sliding scale of state sponsorship—from complete innocence through varying

degrees of passive or active support for cyber attackers to the final level, which is complete control and direction. The tools of law enforcement (i.e., mutual legal assistance and extradition treaties) give way to intelligence operations (such as clandestine surveillance and covert operations) before military options are lawfully available. The fact that non-state actors can cause as much damage as a state actors requires that mechanical applications of simple either/or rule sets be avoided.

The expert members of the legal cell will base their analyses on legal authorities, policy norms, and technological lessons learned. The Schmitt criteria are helpful in integrating these factors. The legal cell will "assign" a group of lawyers to perform their own analysis and compare the results to achieve a better outcome. This is one of the greatest advantages of the legal cell—different lawyers from various organizations in diverse locations working together within the C3IOS architecture in near real time. One, of course, must be designated as the principal legal advisor with the ultimate responsibility for presenting the incident commander with legal advice in time to take effective action.

V. REQUIREMENTS FOR THE VIRTUAL LEGAL CELL

A. STARTING UP

The first step in the authors' requirements analysis was to identify users of C3IOS and other stakeholders whose decision-making or workflow would be affected by the introduction of the virtual legal cell. The authors applied a brainstorming technique to elicit statements from potential users and stakeholders about their perceived needs for legal and policy advice in the decision-making process in the context of conducting cyber warfare operations. From the statements of needs resulting from the brainstorming sessions, the authors identified a set of core or commonly defined needs. They then conducted a use case analysis o determine the context for specifying the requirements for decision-making.

The following questions needed to be answered in order to identify stakeholders and the user requirements:

- Who uses the system (e.g., legal advisors)?
- Who is the customer (e.g., members of the armed forces)?
- Who is affected by outputs of the system (e.g., the decision makers, first responders)?
- Who evaluates/approves the deployment of the system for use?
- Who maintain the system?
- Who else, beyond the primary users can make use of the system (e.g., members of the private sector such as non-governmental organizations, operators of the public infrastructure, companies)?

Stakeholders:	Governmental/political actors; military actors; Judge Advocate General's (JAG) Corps Officers; private sector actors; government/military and legal regulatory teams; law enforcement officers; technologists; technicians; decision makers in government and in all different cells; first responders; and the rest of the systems operators.
Users:	Cyber and Kinetic Warfare Commanders; legal advisors – JAG Officers; cyber warfighters

Table 1. Stakeholders and Users.

In order to elicit valid requirements from stakeholders focused on different levels of expertise, the authors conducted one-on-one in-person meetings and teleconferences with the people who mentored their thesis. Their mentors are subject matter experts—one of the architects of C3IOS, a professor who specializes in the law of information conflict, and a professor who specializes in the technical aspects of cyber warfare—and were able to play the roles of the spectrum of users and stakeholders. The following table contains a summary of the problem to be addressed by the realization of a virtual legal cell.

Element	Description
The problem	Commanders must be able to quickly assess the effects of a cyber attack to determine if their response is 1) A potential use of force that is consistent with a pre-defined set of cyber ROEs, 2) Consistent with a measured response under the International Laws of War, and 3) An appropriate measure of force necessary to counter the initial attacks and their effects? The commander must also determine if perpetrators are legal combatants or criminals, and whether a cyber incident has risen to a level requiring the use of force at all. These decisions must be made at the same operational tempo as the cyber engagements.
Effects	Failure of commanders to address the problem within the framework described above can lead to undesirable legal and political effects with potential consequences in both the national and international arena. Furthermore, cyber operations are conducted around the clock with unpredictable intensity and without regard to the well-defined levels of conflict. For example, the attacks on Estonia resulted in strategic levels of effects, while the traditional level of conflict was characterized as pre-hostilities.
And results in	When this problem is not considered within the problem framework to include the operational tempo and consideration of effects that are less predictable and not consistent with the state of conflict, there is likely to be poor use of human resources; inappropriate responses (e.g., disproportionate use of force); and delayed reactions/responses; incorrect or poorly informed reasoning about the legality of responses to cyber attacks.

Benefits of a solution	The proposed software supports: • legal reasoning in the area of responding to terrorist acts by providing a computer-assisted means for experts to determine whether a terrorist cyber attack has risen to the level of a use of force, with the aim of helping the user reason about the grey areas of the law of information conflict; • information sharing in near real-time among the actors involved in defending cyberspace, with the aim of making recommendations and decisions with a minimum of uncertainty and incomplete information about the situation in the cyber battlespace; • better representation of results, and in this way, better clarification of thoughts for courses of actions and highlighting areas of misunderstanding or disagreement; • effective and legally justifiable responses against cyber attacks; • standardization of the decision-making process. The existence of this system will also allow the more efficient use of human resources.

Table 2. Elements and Descriptions.

The two phases of brainstorming the authors used were idea-generation followed by idea-reduction. The goal was to identify all feasible ideas, focusing on the breadth instead of the depth of the ideas. The authors then used an informal, subjective ‘does-the-idea-have-merit’ test to prune the list of ideas down to a manageable size. Following the technique described in [28], the authors grouped similar ideas together and then ranked each group of ideas as being one of the following: critical, important, or useful. The authors used critical to connote indispensable to the implementation, important to connote a significant loss without a specific feature, and useful to connote nice-to-have. They observed that the most creative ideas resulted from discussions and combinations over unrelated issues with people with different levels of expertise, shown in the table below.

In order to establish the level of effort implied by each feature, the authors determined a rough order of magnitude: low, medium, or high. The risk element is an assessment of the associated risk of each requirement. The prioritization/effort/risk estimations were based on the authors' subjective judgment after interviewing the subject matter experts.

Id	Requirements	Priority	Effort	Risk
Timeliness of response				
001	Agile interactions among the users in the cells.	Important	Medium	Low
002	Real-time response among the different actors.	Critical	Medium	Low
Legal preparedness				
003	Provide a way to support standardization of types of actions by the creation of legal flow charts, to define the criteria and the menu of choices.	Important	Low	Medium
004	Inclusion of templates and pre-planned doctrines, concerning different scenarios, to support the observe-orient-decide-act (ooda) loop.	Useful	Low	Medium
005	Restricted format of actual language to allow communication of technicians with layers, with commanders, with politics and vice versa, with a small set of descriptive words, understandable by all.	Important	Medium	High
006	Capability of storing meaningful laws and books in place ahead of time (constitutional, legislative, executive, judiciary and international).	Important	Low	Low

Dynamic cell and/or static legal cell				
007	Provide capability to distinguish real-time courses of actions.	Critical	Medium	Low
008	Support sharing of information quickly.	Critical	Medium	Low
009	Provide user interface to the appropriate law.	Important	Low	Low
010	Support integration among cyber and kinetic warfare commanders.	Useful	Medium	Medium
011	Should be compatible from an interoperable standpoint with other countries' leaderships systems.	Important	High	High
012	Ability of joining others cells of the system of systems.	Critical	Medium	Medium
012a	Each legal cell shall provide a toolbox with tools to support (analysis) legal work.	Critical	Low	Low
012b	Cells shall operate in a secure environment.	Critical	Medium	High
012c	Provide at least one static legal cell for each major kinetic mission.	Critical	Minimum	Low
Partitioning				
013	The system requires engineering partitioning in order to provide the capability to discriminate what can be done by humans (at lower speed) and what can be done by the system in an automated way (computer executed at high speed).	Critical	Medium	Low
Introduce the framework of Schmitt's analysis				

014	Provide a necessary framework to evaluate whether the attack grows to the level of ‘use of force’ beneath international law.	Critical	Medium	Low
Policies				
015	Necessity to constrain the satisfaction/ realization of pre-existing requirements.	Important	Medium	Medium
016	Should provide a way to discriminate the categorization of legal paradigm (law enforcement, intelligence collection, military operations).	Important	Low	Low
Brokering				
017	Concerning info gathered, the system should have patching capability to hook up intelligence resources and break it down to different services.	Critical	High	Medium
Chain of custody				
018	Should maintain the chain of custody (law to prosecute the attacker and handle evidence, etc).	Important	High	Medium
019	Should log all the actions done in all the cells.	Critical	Medium	Low
020	System should maintain the ability of growing and shrinking according to the demands.	Important	Medium	Medium
Granularity				
021	Should provide discrimination between fine-grained and coarse-grained type of data, in order to define the level of certainty.	Important	Medium	Medium

022	Should provide a way to handle and adjust available sensors [4].	Important	Medium	Medium
HCI				
023	User-friendly context to present data to the lawyers (ensure bright line rules to reduce grey areas) [6].	Critical	High	Low
024	User-friendly context to present legal advice to the others actors.	Critical	High	Low
Usability, extensibility, maintainability and capacity				
025	Should provide web-based and open-source capabilities.	Useful	High	High
Situational awareness				
026	Should provide a way of distributing and publishing data among the users.	Critical	High	High
027	Assess the workload considering task analysis.	Useful	Medium	Medium
027a	Provide cyber sa to legal cells to ensure legal support is aware of changing situations. Sa should be summarized (non-technical as possible) and provide enough detail for lawyers to assess the changing environment and legal implications.	Useful	Medium	Medium

Table 3. Requirements.

Following the approach described in [29], the use case shown in Figure 4 provides the context of the legal cell in terms of actors, their goals (represented as use cases), and the dependencies between those use cases. In the diagram, five critical use cases have been identified and subsequently elaborated with use case scenarios.

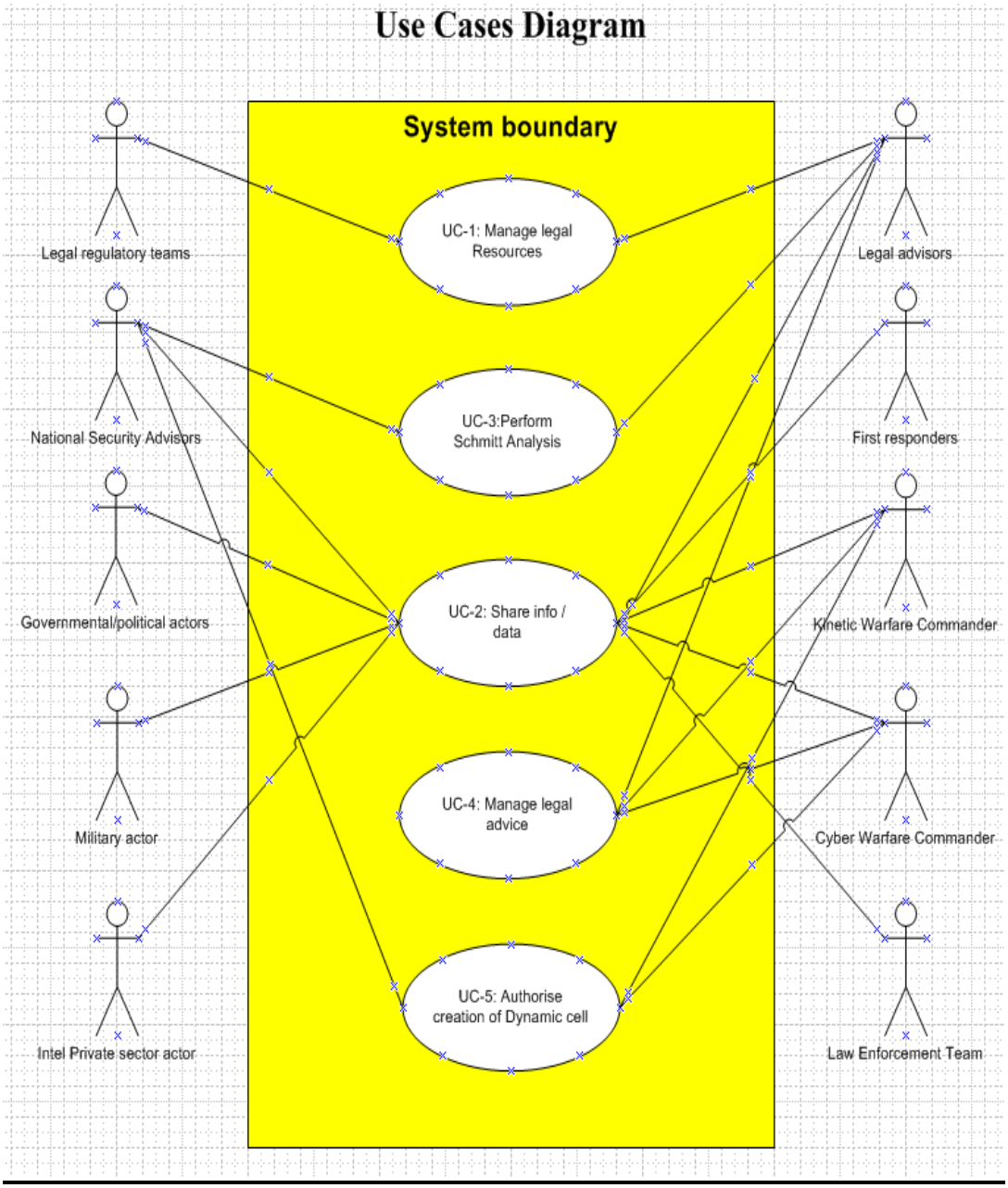

Figure 4. Use Case Diagram for the Legal Cell in C3IOS.

B. EXPANDED USE CASE SCENARIOS

1. UC-1: Manage Legal Resources

Scope: C3IOS

Level: User-goal level

Primary Actors: Legal/national security advisors, legal regulatory team

Secondary Actors: Kinetic Warfare Commander, Cyber Warfare Commander

Stakeholders and Interests:

The Kinetic Warfare Commander, Cyber Warfare Commander, and national security advisors want to have a robust, effective and predictive set of laws in force and embedded in the system's databases to support their future activities/responses by providing the appropriate analysis and decision frameworks for actions.

DIMPLE actors want to have all the necessary tools available to understand, explain and support in the most accurate, secure, timely and flexible way the potential consequences of cyber incidents.

Pre-conditions:

A set of laws will already be available in the C3IOS database.

The legal regulatory teams continuously review and update the legal database to include all the respective laws and relevant case studies to support handling cyber incidents.

The legal advisors of a core or a dynamic cell are logged in and maintain the capability through an easily accessible interface to access information, run analyses, and input their assessments. Legal advisors either in virtual core cells or in dynamic cells are logged in and have authorization to access the databases

to support handling incidents and grounding their assessments of the situation. The legal regulatory team is also logged in to C3IOS either directly or indirectly via remote management software.

The legal database is also available to all the other users of C3IOS, but in order to address administrative issues and protect the confidentiality, integrity, and availability of the data and information system, policy enforcement mechanisms are in place.

Post-conditions:

The legal regulatory team logs out with a fully operational legal database environment established and ready for connection and usage by legal advisors.

Legal and national security advisors can effectively manage to use the system to extract all the updated information in the most direct and appropriate manner.

Main Success Scenario:

1. All the authorized users access the documented database.
2. First responders request support regarding a cyber incident.
3. A member of a CWC cell accesses the area of legal resources.
4. If there are more requests for access, members of the cell repeat step 3.

Alternate Scenario:

3a. If the member of the cell is not authorized to enter legal resources, the access is denied.

Frequency of Occurrence:

For operation and training reasons, qualified members of the various cells maintain the right to access legal resources at anytime.

2. UC-2: Perform Schmitt's Analysis

Scope: C3IOS

Level: User-goal level

Primary Actors: Legal regulatory team

Secondary Actors: Legal advisors

Stakeholders and Interests:

The Kinetic Warfare Commander, Cyber Warfare Commander, and national security advisors want to have a robust, effective and predictive set of legal criteria to determine the level of force applied by an adversary via a cyber incident in order to respond in a lawful manner.

Pre-conditions:

The pre-condition of a certain request for legal advice of a cyber attack follows the implementation of Schmitt's analysis, as a means to assess the attack in terms of the UN Charter. The United Nations Charter clarifies the *jus ad bellum* (the law of conflict management) and the *jus in bello* (the law of war), but it only applies to the countries that ratified this treaty, where the more relevant articles are Article 2(4), Article 39, and Article 51. The goal is to implement a valid procedure to understand the nature of the incident (i.e., is this incident equivalent to an armed attack?) in order to determine the lawful set of responses. The answer is not always clear because a cyber attack can have unintended consequences, possibly even severe, in terms of the quantum of damage. In order to evaluate these consequences, Professor Michael Schmitt created a set of criteria, later refined by Professor Thomas Wingfield, to include not only qualitative but also quantitative measures based in seven different characteristics of an attack: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility.

Post-conditions:

The desired post-condition is the identification of the level of the attack with respect to international law, by the examination of the impact that the incident has in accordance with the evaluation of Schmitt's seven criteria. One initially starts with an incident and then needs to determine if it is an armed attack or something below the threshold of an armed attack. One uses the outcome of the analysis to make and support a decision as to what, if any, level of force to apply in response to the incident. That is, the aim is to provide a systematic and well-grounded means for applying the most appropriate response from the set of available lawful responses permitted by policy.

Main Success Scenario:

1. When a computer network attack is detected, C3IOS will automatically provide legal advisors with a template for conducting Schmitt's analysis.
2. Measure the seven different criteria.
3. Average the values supplied by each legal advisor for each criterion.
4. Based on predefined threshold values for the average values, provide an assessment of whether it is an armed attack.
5. Operator checks the evaluation obtained.
6. Continue to measure the different criteria updates about the incident as they become available (via input to the databases).

Alternate Scenario:

4a. If the value is over the Article 51 threshold, will advise whether an operation constitutes an armed attack, and if so, would permit a use of force in response.

4b. If value is under a determined threshold will not advise the use of force.

5a. If the value changes and is over a determined threshold will advise the use of force.

5b. If the value changes and is under a determined threshold will advise a use of force.

Frequency of Occurrence:

The system will constantly monitor new or preexisting computer network attacks. Each time a virtual legal cell needs to be instantiated to support an exercise or operation, the system will provide the users with assistance in conducting Schmitt's analysis.

3. UC-3: Share Information

Scope: C3IOS

Level: User-goal level

Primary Actors: Legal regulatory Team

Secondary Actors: Legal advisors

Stakeholders and Interests:

The Kinetic Warfare Commander, Cyber Warfare Commander, national security advisors, and DIMPLE actors want to have a robust, effective and predictive set of procedures in force and embedded in the system to support information sharing under need-to-know rules. All the information subscribed to by the actors should be published to them by C3IOS.

Pre-conditions:

Information that can be shared should be readily accessible to all users of C3IOS. The interaction among them should be accomplished as quickly as possible to operate in the direction of near real-time interactions that also maintain response timeliness. The system should enforce need-to-know rules.

Post-conditions:

The desired post-conditions describe near real-time exchanges and sharing of information to support cyber incident evaluation and response procedures. Information needs to be exchanged between different countries, and

between organizations within the same country. A means for brokering information is needed to protect sources and methods while at the same time making information as available as permissible.

Main Success Scenario:

1. The system detects a computer network attack.
2. The system starts to gather information about the attack.
3. The system shares the information.

Alternate Scenario:

3a. If information does not need to be shared deny access to unauthorized users.

Frequency of Occurrence:

This is a cyclical procedure to ensure the timeliness of a response.

4. UC-4: Manage Legal Advice

Scope: C3IOS

Level: User-goal level

Primary Actors: Legal advisors, KWC, CWC

Secondary Actors: Legal regulatory team

Stakeholders and Interests:

This use case describes the steps of the interactive process among the designated actors (KWC, CWC, commanders of the legal cell) under a framework of identified jurisdictions, in order to appropriately support feedback on latent or non-legal issues. The scope is to minimize the grey areas in law and policy to avoid unwitting cross-border consequences during a response to a cyber incident, under the status of national or international law margins. Besides the fact that different nations may adopt variant approximations concerning the way to express their cyber defenses, there are essential characteristics that naturally dictate response behaviors for those types of incidents [23]:

- It is difficult to predefine a specified legal regime for response, since there is no immediate certainty—or sometimes not even an adequate amount of information—about the origin, the level, or the consequences of the cyber incident. One needs the facts before he or she judges the legality of what has or will transpire.
- Member nations of alliances or coalitions should have the ability to coordinate their actions while at the same time retain their own flexibility to respond using the means they deem necessary.
- Global interconnected information and communication Technology (ICT) networks that increasingly support national and international security are structured under wide borders and multiple jurisdictions.

Pre-conditions:

The existence of a database of previous cases is essential to support the managing of the legal advice. By accessing this factual repository of different cases, in combination with the current status provided by the existing laws, the relevant background documentation, and the certainty that gives the level of their expertise, the legal advisors will manage to exchange and receive the necessary level of information to be able to inform the Commander's decisions against cyber incidents.

Post-conditions:

To assist instant information sharing plus sound and valid evaluation of cyber incidents without violating the law and contravening policy, the legal cell can be created for the period that is essential to provide the inevitable support to Cyber Commanders or decision makers, and terminate when the incident and follow-on responses cease. Lawful default responses in accordance with defensive policies, because of the vast legal grey area, are predefined to delimitate bounds within which the responses can be ranged and activated in order to provide the defender more options. By the usage of all the available means, the legal advisors will finally manage the legal advice to support the commander's decision-making.

Main Success Scenario:

1. Authorized users access the documented database.
2. The first responders submit a request for legal advice with respect to a cyber incident.
3. The CWC authorizes the creation of a virtual legal cell and assigns the duty of the commander of the cell.
4. The commander of the virtual cell authorizes membership.
5. A legal advisor accesses the databases in which the data about the incident has been published and performs Schmitt's analyses.
6. The legal cell submits the legal advice and the results of the evaluation under the seven certain quantitative and qualitative aspects of the incident in accordance with Schmitt's analysis.
7. The CWC responds.
8. The CWC authorizes the decommissioning of the legal cell.

Alternate Scenario:

8a. If the operation or the task is not completed a repetition of steps 1-7 exists.

Frequency of Occurrence:

The system supports the formulation of legal advice on a continuous basis.

5. UC-5: Authorize the Creation of the Dynamic Legal Cell

Scope: C3IOS

Level: User-goal level

Primary Actors: Kinetic Warfare Commander, Cyber Warfare Commander

Secondary Actors: Legal/national security advisors

Stakeholders and Interests:

The Cyber or Kinetic Warfare Commanders maintain the right to authorize the creation of a dynamic legal cell to support their assessment when they are facing national incidents or coordinate legitimate international efforts against those types of events under common, consistent jurisdictions.

Each time a commander authorizes the creation of a cell, the cell commander is the one who authorizes membership. The commander who authorizes the cell is also responsible for monitoring—through assured delegation-of-authority procedures—the regular functioning and evolution of the cell and final decommission when the operation is finished. The new cell is at the level of command of the cell commander that permits its formation.

Pre-conditions:

The functionality of the system should support the need of initial actors who will retain the ability to authorize the creation of a dynamic legal cell. It is also necessary to have a pre-established doctrine to ensure timely secure communication capabilities to support the creation of new cells, in addition to a secure procedure for granting membership to a new cell. [10].

Post-conditions:

This virtual legal community, with dynamic interaction, will be able to support the decision-making process used for a specific task or operation and decommissioned after the task or operation is completed [8].

Main Success Scenario:

1. A cell commander (e.g., the CWC of a specific region) requests the creation of a new legal cell for inter-regional collaboration on a problem that currently affects the commander's region.
2. The KWC authorizes the creation of the virtual legal cell and the cell commander for the new cell.
3. A member of the KWC cell monitors the new cell.
4. The commander who authorizes the creation of the legal cell determines the initial membership of the cell.
5. Initial or extra members interact to provide the legal advice.
6. The CWC authorizes the decommissioning of the virtual legal cell.

Alternate Scenario:

4a. If there is no available security clearance for a member to join the cell the access is denied.

Frequency of Occurrence:

Variable, according to the frequency of occurrence of cyber incidents.

C. DISCUSSION OF REQUIREMENTS

In order to revolve the development of the legal cell the authors attempt to clarify and expand the requirements for this cell, focusing heavily on the requirements for the C2 understanding, planning, and deciding activities involved in applying Schmitt's analysis.

1. Legal Foundation for Cyber Warfare

Given the short timeline over which cyber incidents occur, a legal foundation for cyber warfare and the ability to quickly provide legal guidance to commanders while engaged in cyber conflict is a must. Given the evolving international laws pertaining to cyber warfare, commanders need to be cognizant of legal guidelines that could potentially govern the execution of cyber operations and their effects on noncombatants. Since there is little legal reference or precedence for cyber warfare, commanders conducting cyber operations will need routine and continuous legal advice.

Vigorous legal preparedness procedures can release critical thinking and essential creative forces that will explore military, law enforcement, and intelligence issues in order to handle warfighting, legal prosecution, and intelligence gathering activities.

The proposed legal component for C3IOS should allow for the integrated gathering of templates and usage of predefined doctrine, policy, law, and procedures for possible attack scenarios that could unfold. The adoption of relevant procedures ahead of time, combined with an extensive use of pre-accepted criteria as well as a potential menu of choices, will prove highly beneficial for the modeling procedures. Relevant legal flow charts, based on different sets of questions, will also work in this direction, in order to set predefined criteria and a specific menu of choices. In this way, lawful, automated

default responses in accordance with defensive policies in force can be achieved. Due to “the vast legal gray area which exists today operates in favor of the attacker,” a predefined delimitation of those bounds within which the responses can be ranged and activated “would provide the defender with more, rather than fewer, options.” [4]

A requirement is that the applied format should be an intuitively understandable one that effectively bridges the differences with respect to the levels of expertise. There is also a requirement that upon detection of an attack all of the available information (e.g., effects, side effects, origin, and evolution) be disseminated in a usable format to personnel with no special technical skills. They will analyze/evaluate the reality of the situation and propose/discuss the action that needs to be taken.

The case of Estonia constitutes a persuasive example, since it is highly reliant in all aspects of society on information technology. Estonia was the first country to use online voting, have almost all government agencies virtually connected, and rely almost exclusively on electronic payment and banking. At the same time, such an infrastructure provides a tempting target for malefactors who are intent on disrupting society. During the Bronze Soldier attacks of 2007, even when the consequences were more than obvious, the Estonian government was not adequately prepared to gather, process, disseminate, and act upon data about the attacks, which also left their legal experts in a position of providing advice based on uncertain and incomplete information. To the authors’ knowledge, there was no system like C3IOS in place to support the defenders. In this direction, the authors conclude that the derived requirement demands the usage of a restricted subset of natural language, which will allow the automated management and flow of information among the users, based on a limited set of descriptive words understandable by all users of C3IOS.

> Efficient cyber security and defense requires an understanding about the cross-border of cyber threats, and the necessity to clearly defining, legally establishing, and regularly exercising policies and practices for cyber incident management. Those policies need to

include joint public and private sector responsibilities as well as the necessary international collaboration. The legalities and political ramifications of cyber security defense and response options need to be predefined at all relevant levels within military and civilian security departments, law enforcement and intelligence offices, information and communications technology companies, foreign affairs agencies, and international alliances and organizations. [30]

2. Dynamic and Static Cells

To reach consensus on what actions to take in response to an attack, there is a requirement to retain the legal expertise in the field. The great uncertainty on the cyber battlefield in addition to the commander's need to be always legally advised mandates the existence of these legal cells, which brings close to the field a wide range of legal expertise in fending off relevant incidents and supports the appropriate procedures that should be followed, taking into consideration the complex legal perspective. Up until now, it is that the assistance is offered by the physical existence of the respective personnel to the core/static cells of cyber and kinetic commanders.

There is a requirement that static cells should be assigned at least per major kinetic mission, manned with a round-the-clock watch jointly by experts from key sectors to assure adequate legal assurance. The dynamic cell should be created in the base of eventuality of occurrence to assist cross-domain incidents and terminated afterwards.

What is proposed for this new legal component of the system is, in addition to the static cells, the introduction of a new dynamic cell that is able to support all the previous tasks and address the demanding cross-domain information sharing and collaborative requirements. "A full understanding and effective response may only be possible by bringing information from those various sources together for the benefit of all." [31] The analysis and response, especially to the cross-border cyber incidents, requires high-level coordination and modulation of actions among different governmental and other organizations of the nations based on interpretation of cyber actions in accordance with the

respective set of laws in force. An obvious problem is that those interpretations, or even the terminology that is in force, might differ significantly from one nation to another.

> Article 25 of the European Union (EU) Data Protection Directive permits the transfer of Personable Identifiable Information (PII) to a non-EU country only if the European Commission has determined that the non-EU country ensures an adequate level of protection. As a whole, U.S. privacy and information protection law does not meet the Commission's standards. However, EU PII can still be shared with the United States under certain contractual arrangements by which the receiving U.S. entities agree to data processing and sharing constraints that meet the *Data Protection Directive's* requirements. For example, air carriers operating flights to or from the United States or across U.S. territory have contractual agreements that permit the carriers to share EU passenger name records (PNR) data with U.S. customs authorities. In addition, U.S. entities that voluntarily certify to the U.S.-EU Safe Harbor Framework may receive EU PII. Many non-EU countries—such as Australia, Argentina, Canada, and Switzerland—have adopted privacy laws similar to the EU's law. [32]

To assist timely information sharing as well as sound and valid evaluation of cyber incidents without violating these legal requirements, the proposed legal cell must be persistent; that is, available for the duration in which the decision makers need to use the cell. There is also a requirement to terminate legal cells when they are no longer needed, such as the conclusion of a conflict or when the creation of a new cell makes an existing cell redundant. Upon termination of a cell, there is also a requirement that the information processed by that cell be archived for future use in operations, training, studies, and investigations.

Another requirement for the system is to provide the capability to distinguish and support real-time course-of-action formulation and execution. Thinking in terms of the 'Cube' [33] described by Thomas C. Wingfield and Eneken Tikk—technological (the "possible"), legal ("permissible"), and policy (the "preferable") dimensions in cyber warfare operations—"allows us to organize the process of cyber security implementation as opposed to the substance of cyber security" [33] Wingfield and Tikk's 'Pyramid' [33] provides a way to categorize

three different types of responses against a cyber attack, based on the preferable/allowed time of the response. The approach involves distinguishing between actions that should be adopted immediately—almost supported by automated procedures—and reactions that might be taken after some consideration. Presumptions are “binary” yes-or-no rules based on predefined criteria and planned countermeasures that aim to support the first responder’s automated reaction. Algorithms can also be executed by an automated system, but it instantiates a parallel decision-making path to indicate the type or the level of extra defensive actions that need to be taken. The law defines time-consuming actions that must be supported by an extensive decision-making procedure. This type of response refers to cases in which the decision maker cares more about the quality of the advice than the timeliness of the response. Finally, the ‘Screen’ [33] identifies an easily accessible user-friendly HCI, which integrates a huge repository of data easily accessible by the respective humans involved in cyber incident management. The three proposed constructs by Wingfield and Tikk should be incorporated into C3IOS since they “represent the *status quo* of cyber security law and policy, and highlight issues relevant for regulatory and policy authorities at the international, national, and private enterprise levels.” [33].

Another critical constraint should be the ability to maintain integration among other vital cells of respective commanders and decision makers to support integrated cyber/kinetic operations, testing and training. Even though the notion of a dynamic cell is a feature already embedded in the architecture of C3IOS, one needs to identify it as an essential characteristic to achieve efficient interaction among the wide range of types of expertise needed to fend off cyber attacks. These include at a minimum the categories of stakeholders called out in the DIMPLE model [30]: diplomatic corps, intelligence community, military, politicians, legal community, and economy community. This requirement is already met by C3IOS, except for providing explicitly tailored support for the legal community.

3. Human Computer Interaction

Requirements placed on the Human Computer Interface (HCI) for C3IOS are of paramount concern, as the main aim of the system is to support collaboration and communication among humans. C3IOS already has a toolbox-like capability for customizing the presentation of data to the needs of the different types of stakeholders.

“Although perfect real-time knowledge of all cyber threats is an impossible goal, it is realistic to do much better at providing a richer, better integrated picture of our cyber security to the technologists, attorneys, and political leaders who will have to collaborate to avert the next cyber attack.” [33] The notion of the ‘Screen’ presented by Thomas C. Wingfield and Eneken Tikk can be very helpful to define the HCI. There is a requirement that the cell provide users with the ability to access “educational materials, lessons learned, and white papers, as well as relevant legal and policy instruments, providing experts and decision-makers with up-to-date and quality instructions on different aspects of cyber security.” [33]

The HCI also needs to provide a clear picture of the context of discourse in a collaboration to support identifying the relevant bright line rules and reducing grey areas of the law even with imperfect knowledge of the current situation. On one hand, one wants to have an efficient comparative framework that will allow first responders to communicate in a timely and understandable manner the information about a cyber incident while at the same time making it possible for the legal experts to do likewise for the benefit of the first responders and the other stakeholders [8].

Tikk et al. provide use with some examples of the confusion that might occur among different actors when interpreting the term “cyber attack.” The actual incident may only involve distributed denial-of-service attacks concentrated on a few networks, or it could mean in another instance a large-

scale, well-organized campaign with far reaching consequences. The choice of words is important when dealing with stakeholders because they each come with preconceived notions of what the terms mean. Tikk goes on to write

> The term ‘cyber security’ is currently used in the United States (US) legislation (e.g. Cyber Security Enhancement Act of 2002), whereas the European Union (EU) refers to terms such as network and information security (NIS), information and communication technology (ICT) security, information technology (IT) security, information security, network security, etc. [34]

Conversely, “a uniform understanding of the details of cyber incidents would promote expert discussions in the field and avoid parallel vocabulary on the topic of common concern.” [34]

Another facet of the HCI is usability, which is concerned with how easy interfaces are to use and the methods to improve the use of the system. Usability is defined by the following: learnability (i.e., accomplish basic tasks in a first approach), efficiency (i.e., perform tasks after understanding the design), memorability (i.e., after being away from the system, how easy is to start using correctly), errors (i.e., how bad errors are and how difficult is to recover from them), and satisfaction (i.e., how pleased the users are). There will be derived requirements for usability such as providing online help to assist users in understanding what functionality is available to them in the legal cell and how to use that functionality.

4. Timeliness of Response

“Timeliness” is highly related to “window of opportunity,” which is the measure of how time is managed; in other words, time between the occurrence of an event and when actions are taken. A “system response time” is the total elapsed time between the received stimulus and the delivered response. This stimulus usually contains a lot of uncertainty, and any decision should be delayed until this uncertainty is lowered to an acceptable threshold (the more time spent

to reduce uncertainty, the longer the response time), as a certain option make take more time but can have a more desirable result with something called “quality of option.”

The right response at the right time is about tempo (“The tempo tells us how complex an environment the system can handle, while the response time tells us when it responds in time,” [35] and is critical when some type of incident or mishap is about to occur. After an attack, there are actions that need to be taken, and the time to take them is vital in the development of a response. Nevertheless, pre-actions should exist in order to help to accelerate these responses. There is never an answer to everything; time is needed to react and to make decisions in different situations.

Two important requirements should be introduced related to agile interactions among the users in the cells and a timely response among the different actors. The mode to establish the interactions among the users is a meaningful step for the C3IOS system; users of C3IOS can instantiate and join cells at any time to collaborate. When an attack happens, automated actions with no immediate human oversight (reflecting unambiguous determinations of lawful conduct for defense against any potential intruder) are taken. The automated proxies for the human first responders can respond based on measures in black or white if-then rules and algorithms built into the system (i.e., decisions based on objective criteria). The human first responders must monitor the situation and take action when the automated system cannot respond on its own or the system takes or may take an incorrect, ill-advised, or unlawful action. Thus, the actions of the humans will contribute to the lumped lag (i.e., the sum of the delays) in responding to any stimulus. Thus, there is a requirement for the C3IOS operational and system architectures to support rapid legal analysis and response within the cyber C2 OODA loop.

There are human factors that need to be taken into account in partitioning the system into its automated and manual pieces [36]. For example, compatibility, which refers to relations among control and displays, affects how

an input will be received, processed, and finally selected in the course of action. One must also consider that the human operator's can speed the learning, and the reaction processes, with fewer errors. As another example, consider processing time, which is the time a person takes to process information. These times range from one person to another and vary according to the complexity of the processing task. As a third example, human operators can become overloaded with information and as a result fail to complete their tasks on time or correctly. There will be derived requirements tied to the performed tasks to better understand the needs of the human users of the virtual legal cell.

5. Schmitt Analysis Framework

There will be derived requirements for supporting the information collection, processing, and dissemination related to each of the seven criteria used in the Schmitt analysis, as well as the collaboration between the lawyers to develop qualitative rankings for each criterion, translate the qualitative rankings into qualitative values, and reach a consensus on whether this is an armed attack.

6. Policies

As mentioned by Lessig [37], there are four aspects in the regulation of cyberspace:

- The laws, created by governments with the objective of sanctioning and forcing;
- Social norms, based on expectations of encouragement or embarrassment;
- Markets, regulated by price and availability;
- And architecture, what is feasible in relation to technology.

A policy can be raised from governance, which grounds collective choice and efficiency. According to [38],

> A single policy must be set that cannot help but affect all those within the scope of the community. Varied preference values must be aggregated such that the single value is acceptable and

> considered legitimate by the community…Even when individuals can act upon their individual preferences (values), an aggregate value set by a central institution may be more efficient or rational over a longer time frame for the individuals of the community. In such cases, it is useful for a central authority to establish a single value rather than (1) requiring each individual to undertake the transaction cost of negotiation, or (2) permitting market failures and short term irrationality.

Policy is a plan of actions to steer choices and attain a coherent result, or what is done continuously even without any plan. It is also choice between decisions, discriminating the costs and priorities, in consideration of the impact they will have on the behavior of the system. Policy specifies the latitude decision makers have in applying the law. Thus, there is a requirement that the legal cell inform the users of the policy that is applicable to the law.

7. Brokering

Understanding that cyber conflicts can be borderless, regional, national and international, security must be addressed. As stated in the *Cyber Security Collaboration Report* of May 21, 2009*,* "operational collaboration enabled by strong, effective information sharing, which is vital in a cyber threat environment that is relentless and increasing in scope," [32] the triumph on these types of situations depends on the degree of using and information sharing.

At the 2009 Cyber Conflict Legal and Policy Conference, there was discussion that the legal and policy framework should be characterized by a comprehensive and multidisciplinary approach that incorporates legal measures for the prevention and response to cyber threats as a cross product of international collaboration and cooperation [30]. This should be accomplished without neglecting national limitations of private sector legal rights and responsibilities for the ICT systems [30]. To realize such a goal the cells and C3IOS as a whole must be trusted to enforce confidentiality, integrity, availability and other security policies. The challenge is to provide an adequate level of trust in a cross-domain information-sharing environment.

Information brokering is about getting the right information to the right people at the right time, Not everyone involved in responding to a cyber incident needs to know everything about the incident. The system needs a capability to control access and operations on data, in a role-by-role basis. Given the sheer number of people involved in responding to a cyber incident, it would not be practical to administer access rights on an individual-by-individual basis.

Technologically speaking, what is needed is for C3IOS to be a high-assurance system that provides for cross-domain multilevel security (CDMLS) [39]. C3IOS has some of the attributes of cloud computing, including dynamic provisioning, which raises many issues of trust [40]. Thus, there will be derived security requirements for C3IOS.

There are laws in place like the *2003 Legislative and Regulatory Task Force Report* [41] or the *Sherman Antitrust Act of 1890* [42] between different countries, the *2007 NSTAC Report to the President on International Communications* [43], and Article 25 of the European Union (EU) *Data Protection Directive.* There are also liability protection models like *The Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act)* [44] and *The Year 2000 (Y2K) Readiness and Responsibility Act of 1998* [45]. C3IOS already has mobile agent patrols (i.e., dynamic sensors) that can be used to construct lawful plans in order to help control and search for information relevant to an incident.

As mentioned in the references above, cross-domain involves dissemination of info across multiple security levels, organizational boundaries, and information systems (e.g., “Intelligence Community (IC) currently classifies information to protect the sources and methods of its intelligence collection activities. The IC is therefore reluctant to share detailed cyber security threat data, fearing that the private sector may not adequately protect the sources of this information…” [32]), and the same fears will be felt in the international

community. To repeat, trust relations and safe ways of communication have to be addressed, not to jeopardize the sources and the methods of collection, processing, and dissemination of information.

8. Granularity of Information

There is a requirement to be able to control the networks of different types of sensors available in C3IOS to ensure that the users of C3IOS can obtain information at the appropriate level of granularity for the decision-making task at hand in the legal cell. For example, to obtain a fine level of granularity, a user may need to focus all of the available sensors on a particular object or area of interest in cyberspace. C3IOS provides for:

- Static sensors (intrusion detection systems (IDS), firewalls, tripwire, etc.)
- Mobile agents (sensors) tuned to look for a specific direction or task to accomplish. They are lightweight agents that are dispatched to other machines/areas in order to drill down and collect information. This information is published (it does not matter where it comes from, but if it is needed to the rest of the cells) respectively to other cells and to their one cell (commander).

Another requirement is to have the system assist the user in setting the granularity through automatically making adjustments or making recommendations to the user. In order to meet timeliness requirements, one must match the level of granularity of information to the time allotted for making a decision. For example, for situations in which the response must be made quickly, the sensing can be set for coarse granularity: there is no time for the human or system to wait for or process fine levels of information. In addition, the system will need to take into account the tradeoff between speed and the risk of making the wrong decision based on using a suboptimal level of granularity. For example, if the legal experts must make a decision whether to launch a counter attack, they may need to take additional time and obtain a fine level of information. By doing so, it minimizes the risk that the commander will make a decision that results in actions that fall in the category of cyber war crimes (e.g.,

application of a disproportionate level of force). In other words, the requirement here is to “gain a competitive advantage over its opponent by reducing in some way the timeliness, accuracy, or precision of data and information utilized by the software agents on the targeted cooperative engagement grid.” [46]

9. Scalability, Availability, Maintainability, and Survivability

The legal cell will need to be able to scale in size as users join and leave the cell. C3IOS will need to be able to handle the growth in the number and size of legal cells in addition to the needs for communication, processing, and storage capacity.

Maintainability is concerned with the ease and speed with which a system can be restored to operational status after a failure occurs. Availabilty is concerned with system-up time. Survivability is concerned with being able to continue to operate under adverse conditions. The legal cells must be highly available, maintainable, and survivable. Given the high tempo of cyber battle, even a short period of unavailability of the system would be unacceptable. The attackers may even try to attack C3IOS itself. Thus, C3IOS must have its own defenses in order to survive attacks, and such defenses are already available in C3IOS.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. SUMMARY

Integrated C2 systems for use in cyberspace are needed because conventional C2 systems are tailored to the requirements for kinetic warfare and not cyber warfare. Cyber attacks can target multiple organizations concurrently, so there is a need to provide information sharing, coordination of COA, situational awareness, and other C2/BM capabilities both within and across administrative domains. C3IOS is such a prototype C2/BM system; however, at present it does not include a means for facilitating the participation and assessment by legal experts in regards to the lawfulness and policy implications of a proposed COA. Decisions made solely on local information in large-scale distributed systems are not optimal and may result in unintended or unwanted results, such as the commander taking unlawful action that makes him or her a war criminal or a civilian a criminal. Thus, there is a need for computer-assisted legal reasoning for distributed C2/BM in cyber operations to enhance the ability of defenders to obtain legal advice about a COA in a short enough time window to keep OODA loops less than or equal to that of the attackers.

In this thesis, the authors proposed the addition of a virtual dynamic legal cell to C3IOS. One of the challenges in cyberspace is to identify or define a hostile act and the subsequent use of force against it. The legal cell will support the cyber warfare activities by providing a qualitative and quantitative grounding, taking into consideration the legal perspective. This cell will act as a means for defenders to engage experts in the law of information conflict to assess proposed COAs. Among other things, the legal advice community will maintain a library of laws and policies, guidance given in past operations, and other information that will be useful to the commander and his or her team of defenders. This cell will use the same type of decision trees used today by attorneys, based on verifiable

criteria, without losing human reflection and creativity by using synchronized actions to ensure the maintenance of capable software and hardware resources to carry out the operations.

Initially, the legal advice team is created with legal experts that will review the data provided to them by C3IOS about the cyber incident. In the authors' case study, they envision that the legal experts will check and analyze the sources of evidence for the event by engaging Schmitt's analysis and finally determine if there is any reason for the use of force under international law. The final product is the creation of a legal basis for a particular type of response to the attack, presented in a format tailored to the needs of the decision maker and authorized members of the cell in order to support their ability to react rapidly to an attack as the attack progresses.

The authors developed a set of requirements for the Virtual Legal Cell via the use of brainstorming among the authors, an academic cyber researcher, a C2 structure expert, and an attorney who specializes in the law of information conflict. The authors also conducted role playing (e.g., warfighter, policy maker). The first step in the requirements engineering exercise was to identify the stakeholders and users of the system. Within the boundaries of the three critical dimensions in cyber warfare operations—the possible, the preferable and the permissible—the goal was to identify the initial set of requirements. The authors relied on simple direct interviewing using context-free questions to elicit the requirements and generate ideas, followed by the application of idea-reduction techniques. The requirements were grouped by the usage of similarity criteria and prioritized with the following rankings: critical, important and useful. Critical means indispensible, important refers to loss significance, and useful is nice-to-have implementation wise. Moreover, the level of effort was established and risk associated with each one of the requirements based on the authors' subjective judgment was assessed. Lastly, the authors expanded each of the requirements in order to clarify the understanding, planning, and deciding activities as they pertained to the legal cell.

B. FUTURE WORK

This core set of capabilities is just a first approximation that will change over time when the virtual legal cell will be made available to the community. The users will likely identify additional requirements for the legal cell and C3IOS, so a plan needs to be developed for the evolution of C3IOS. In addition, validation of the requirements still needs to be done.

The virtual cell will have to continuously enhance the communication and decision-making processes. More research needs to be done on the underlining distributed system messaging of publish/subscriber versus request-reply, which is more relatively delayed on large global networks than on the actual communication themselves. Publish-and-subscribe communications are used to create real-time custom signatures for specialized tasks. They are implemented by broadcast usage rather than multicast techniques, since the subscriber does not need to know where the publisher is located, and conversely the publisher does not need to know where the subscriber is either. The advantage of C3IOS in terms of speed and performance comes from its peer processing architecture that does not need to go across the network to get data, but as soon as user subscribes the data it becomes available to the whole community of users, which minimizes the processing, messaging and data acquisition. The applied models or approaches are the notions of dynamic system reconfiguration, honeynets, mobile agent patrols, secure publish/subscribe communication protocols, movement of state, and virtualization for deception purposes. The current status of C3IOS is a distributed cyber C2 system that can be tailored and deployed across any enterprise, or even the national communications infrastructure and the global information grid. Send and receive messages with the community members and authorized members of other cells, is a major research issue. A constrained natural language needs to be developed to support information sharing.

The cell has to implement provide for decision trees to increase the speed of the decision making process, based on objective verifiable criteria, without losing human reflection and creativity [4]. This standardization of the decision-making process can be done with algorithms that can be executed by an automated system and also support those tasks that are human-centered, in particular those that are carried out to address gray areas of the law and the consideration of policy.

C3IOS technology has to accommodate and easily integrate either civilian or military organizations, so they can both use this technology and the operational model at the same time in an effective manner. The proposed legal cell can be used by either the military or private sector, because it will provide legal reasoning regarding what the organization can do to protect itself. This is a key point, since cyber warfare is not a military activity alone, as the military also uses civilian critical infrastructure. C3IOS architecture offers the ability to deploy cells on both the military and the civilian side, so the study of the better architecture that will facilitate this integration is also a great research area.

On the other hand, there needs to be information sharing, as defined in the requirements. Proper information sharing, which is the right amount to deal with the threat and create mitigation measures but at the same time protect the methods and sources, is a very sensitive field. Information sharing plus sound and valid evaluation of cyber incidents without violating security policy is essential to provide the inevitable support to Cyber Commanders' or decision makers. Lawful default responses in accordance with defensive policies, because of the vast legal gray area, should be predefined to delimitate bounds within which the responses can be ranged and activated in order to provide to the defender more options.

Of course, a next step is to build a prototype of the legal cell and have users of C3IOS try out and provide feedback about the cell. Here is will be important to capture the complexity and nuances of diverse national approaches to warfighting and more specifically requirements for computer-assisted legal support for decision making.

Additional research is needed on protecting C3IOS from being manipulated by an attacker in a spy-versus-spy manner. For instance, how could C3IOS be strengthened so that misinformation provided to the system can be detected, flagged and reported to the users of the legal cell?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1]. F. Burton and S. Stewart, “Threats, Situational Awareness and Perspective,” *stratfor.com*. [Online]. Available: http://www.stratfor.com/threats_situational_awareness_and_perspective [Accessed Jan. 14, 2010].

[2]. Wikipedia, “NASA,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/NASA [Accessed: Jan. 13, 2010].

[3]. N.R. Howes and J.Sarkesain, “Dynamic Virtual Communities and Mobile Agent Architecture,” in *3rd Annual IEEE Information Assurance Conference*, West Point, NY, 2002.

[4]. T. C. Wingfield, J. B. Michael, and D. Wijesekera, “Optimizing Lawful Responses to Cyber Intrusions,” *dodccrp.org* [Online]. Available: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/290.pdf [Accessed: Nov. 12, 2009].

[5]. Wikipedia, “International humanitarian law,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/International_humanitarian_law [Accessed: Jan. 10, 2010].

[6]. D. E. Denning, “The Ethics of Cyber Conflict in Information and Computer Ethics,” *faculty.nps.edu* [Online]. Available: http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf [Accessed: Oct. 21, 2009].

[7]. J. B. Michael, T. C. Wingfield, and D. Wijesekera, “Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System,” in *Proc. Twenty-seventh Annual Int. Computer Software and Applications Conf., IEEE,* 2003.

[8]. Institute for Defense Analysis, *National Aeronautics and Space Administration Cyber Operations Information System (COIS) Cyber Warfare Command, Control, Communications, Computers, Intelligence and Operations (C4IO),* Institute for Defense Analysis, Dec. 2004.

[9]. V. K. Garg, *Elements of Distributed Computing*. Wiley & Sons, 2002.

[10]. The Free Dictionary, “computer network defense,” *thefreedictionary.com*. [Online]. Available: http://www.thefreedictionary.com/computer+network+defense [Accessed: Feb. 10, 2010].

[11]. N. Howes, M. Mezzino, and J. Sarkesain, “On Cyber Warfare Command and Control Systems,” *9th Annual International Command and Control Research & Technology Symposium*, 2004, http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/118.pdf [Accessed: Sep. 5, 2009].

[12]. Wikipedia, “Honeypot (computing),” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/Honeypot_(computing) [Accessed: Jan. 10, 2010].

[13]. N. C. Rowe, “Designing Good Deceptions in Defense of Information Systems,” in *Proceeding of the 20th Annual Computer Security Applications Conference, IEEE*, 2004, pp. 418–427.

[14]. Honeynet Project, “Know Your Enemy: GenII Honeynets,” *honeynet.org*. [Online]. Available: http://old.honeynet.org/papers/gen2/ [Accessed: Jan. 11, 2010].

[15]. Wikipedia, “Mobile agent,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/Mobile_agent [Accessed: Jan. 20, 2010].

[16]. J. B. Michael, G. Fragkos, and M. Auguston, “An experiment in software decoy design: Intrusion detection and countermeasures via system call instrumentation.” In D. Gritzalis, S. D. C. di Vimercati, P. Samarati, and S. Katsikas, Ed. *Security and Privacy in the Age of Uncertainty*. Norwell, MA: Kluwer Academic Publishers, 2003, pp. 253–264.

[17]. N. Howes, M. Mezzino, and J. Sarkesain, “Cyber Warfare Command and control,” *dodccrp.org*. [Online]. Available: http://www.dodccrp.org/events/9th_ICCRTS/CD/presentations/7/118.pdf [Accessed: Dec. 10, 2009].

[18]. Wikipedia, “Global Information Grid,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/Global_Information_Grid [Accessed: Jan. 15, 2010].

[19]. Charter of the United Nations, “Chapter I: Purposes and Principles,” *un.org*. [Online]. Available: http://www.un.org/en/documents/charter/chapter1.shtml [Accessed: Jan. 20, 2010].

[20]. Charter of the United Nations, “Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression,” *un.org*. [Online]. Available: http://www.un.org/en/documents/charter/chapter7.shtml [Accessed: Jan. 5, 2010].

[21]. M. N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, *37 Columbia Journal of Transnational Law 885-937* , reprinted as *Institute for Information Technology Applications (USAF Academy) Publication # 1*, July 1999.

[22]. Federation of American Scientists, “Department of Defense Directive,” *fas.org*, May 9, 2006. [Online]. Available: http://www.fas.org/irp/doddir/dod/d2311_01e.pdf [Accessed: Jan. 11, 2010].

[23]. ePractice, “eGovernment Factsheet - Estonia - History,” *epractice.eu*, Jan. 13, 2010. [Online]. Available: http://www.epractice.eu/en/document/288214 [Accessed: Jan. 25, 2010].

[24]. Wikipedia, “2004 Madrid train bombings,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/2004_Madrid_train_bombings [Accessed: Jan. 3, 2010].

[25]. Wikipedia, “7 July 2005 London bombing,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/7_July_2005_London_bombing [Accessed: Jan. 14, 2010].

[26]. Wikipedia, “Sarin gas attack on the Tokyo subway,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/Sarin_gas_attack_on_the_Tokyo_subway [Accessed: Jan. 20, 2010].

[27]. Wikipedia, “repsia loquitur,” [Online]. Available: http://en.wikipedia.org/wiki/Res_ipsa_loquitur, [Accessed: Feb. 20, 2010].

[28]. D. Leffingwell and D. Widrig, *Managing Software Requirements, Second Edition, A Use Case Approach*, Addison-Wesley Pearson Education, 2003.

[29]. Wikipedia, “Use case diagram,” *wikipedia.com*. [Online]. Available: http://en.wikipedia.org/wiki/Use_case_diagram [Accessed: Jan. 10, 2010].

[30]. CCD COE, “International Cyber Conflict,” presented at Legal & Policy Conference 2009, Tallinn, Estonia, 2009.

[31]. National Defense Industrial Association, “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,” *ndia.org*, 2009. [Online]. Available: http://www.ndia.org/Advocacy/PolicyPublicationsResources/Documents/Cyberspace_policy_review_2009.pdf [Accessed: Jan. 29, 2010].

[32]. The White House, “NSTAC Response to the Sixty-Day Cyber Study Group,” *whitehouse.gov*, May 21, 2009. [Online]. Available: http://www.whitehouse.gov/files/documents/cyber/NSTAC%20Response%20to%20the%20Sixty-Day%20Cyber%20Study%20Group%203-12-09.pdf [Accessed: Jan. 26, 2010].

[33]. T. C. Wingfield and E. Tikk, “Frameworks for international cyber security, the cube the pyramid and the screen,” unpublished manuscript, 2009.

[34]. E. Tikk and M.Jur, “The DIMPLE Approach to International Cyber Conflict,” *The Center for Infrastructure Protection (CIP) Report*, vol. 7, no. 11, May 2009.

[35]. P. Cothier, “Access of Timeliness of Command and Control,” dspace.mit.edu. [Online]. Available: http://dspace.mit.edu/bitstream/handle/1721.1/15420/12731523.pdf?sequence=1 [Accessed: Mar. 3 2010].

[36]. M. Sanders and E. McCormick, *Human Factors In Engineering and Design,* McGraw-Hill United States of America, 1993.

[37]. L. Lessig, “The Laws of Cyberspace”, *lessig.org*, 1998. [Online]. Available: http://www.lessig.org/content/articles/works/laws_cyberspace.pdf [Accessed: Jan. 27, 2010].

[38]. J. Reagle, “Why the Internet is Good,” *cyber.law.harvard.edu*, 1998. [Online]. Available: http://cyber.law.harvard.edu/archived_content/people/reagle/regulation-19990326.html [Accessed: Dec. 5, 2009].

[39]. IEEE Xplore Digital Library, “Using RuleML to specify cross-domain information flow control policies,” *ieeexplore.ieee.org*. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5282339&isnumber=5282304?tag=1 [Accessed: Jan. 10, 2010].

[40]. J. B. Michael, “In Clouds We Shall Trust,” *IEEE Security & Privacy*, vol. 7, no. 05, pg. 3, Sept./Oct. 2009.

[41]. National Security Telecommunications Advisory Committee, *NSTAC LRTF Report: Barriers to Information Sharing*, Sept. 2003.

[42]. Unite States Congress, *Sherman Antitrust Act of 1890, July 2, 1890, ch. 647, 26 Stat. 209, 15 U.S.C. § 1–7*, 1890.

[43]. National Security Telecommunications Advisory Committee, *NSTAC Report to the President on International Communications*, Aug. 16, 2007.

[44]. United State Congress, *Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, 6 U.S.C. §§ 441-44 (2006)*, 2006.

[45]. United States Congress, *Year 2000 (Y2K) Readiness and responsibility act of 1999, Public Law 106-37*, 1999.

[46]. J. B. Michael, “On the Response Policy of Software Decoys: Conducting Software-based Deception in the Cyber Battlespace,” in *Proceedings of the Twenty-sixth Annual Computer Software and Applications Conference IEEE,* Oxford, England, Aug. 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information *Center*
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Prof. James Bret Michael
   Naval Postgraduate School
   Monterey, California

4. Prof. Thomas C. Wingfield
   George C. Marshall European Center for Security Studies
   Garmisch-Partenkirchen, Germany

5. Mr. John F. Sarkesain
   Aerospace Corporation
   Washington, D.C.

6. Hellenic Navy General Staff
   Athens, Greece

7. Portuguese Navy General Staff
   Lisbon, Portugal

8. Georgios Dementis
   Naval Postgraduate School
   Monterey, California

9. Gonçalo Sousa
   Naval Postgraduate School
   Monterey, California