NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NEXT GENERATION ENTERPRISE NETWORK BUSINESS CONTINUITY: MAINTAINING OPERATIONS IN A COMPROMISED ENVIRONMENT

by

Erik C. Hansen

March 2016

Thesis Advisor:	Albert Barreto III
Second Reader:	Man-Tak Shing

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 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE NEXT GENERATION ENTERPRISE NETWORK BUSINESS CONTINUITY: MAINTAINING OPERATIONS IN A COMPROMISED ENVIRONMENT			**5. FUNDING NUMBERS**
6. AUTHOR(S) Erik C. Hansen			
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. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Operation Rolling Tide, and the events that led up to its initiation, highlighted certain areas in Navy network operations that needed improvement, including maintenance of command and control (C2) of a compromised network. The current continuity of operations plan for NGEN does not detail a contingency providing high-fidelity C2 of the enterprise in the event of an intentional compromise.

Evaluating published literature on virtualization, available technology products currently on the market, and tactics for employing virtualized environments, this research explores whether virtualization is able to provide options allowing network operators to maintain positive C2 during a compromise. It also examines if virtualization will scale appropriately for use in enterprise networks in terms of monetary and manpower costs, and any return on investment that may be realized.

Using virtualization technology to create a tailored space capable of collaboration and network modelling provides an option for maintaining secure and useful C2 of the network. The costs involved, if implemented in the current NGEN contract, equate to approximately one-tenth of one percent of the contract award. The primary return on investment is increased readiness.

14. SUBJECT TERMS Continuity of operations, business continuity, virtualization, Next Generation Enterprise Network, NGEN			**15. NUMBER OF PAGES** 59
			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. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

NEXT GENERATION ENTERPRISE NETWORK BUSINESS CONTINUITY: MAINTAINING OPERATIONS IN A COMPROMISED ENVIRONMENT

Erik C. Hansen
Lieutenant, United States Navy
B.A., San Diego State University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2016

Approved by: Albert Barreto III
Thesis Advisor

Man-Tak Shing
Second Reader

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Operation Rolling Tide, and the events that led up to its initiation, highlighted certain areas in Navy network operations that needed improvement, including maintenance of command and control (C2) of a compromised network. The current continuity of operations plan for NGEN does not detail a contingency providing high-fidelity C2 of the enterprise in the event of an intentional compromise.

Evaluating published literature on virtualization, available technology products currently on the market, and tactics for employing virtualized environments, this research explores whether virtualization is able to provide options allowing network operators to maintain positive C2 during a compromise. It also examines if virtualization will scale appropriately for use in enterprise networks in terms of monetary and manpower costs, and any return on investment that may be realized.

Using virtualization technology to create a tailored space capable of collaboration and network modelling provides an option for maintaining secure and useful C2 of the network. The costs involved, if implemented in the current NGEN contract, equate to approximately one-tenth of one percent of the contract award. The primary return on investment is increased readiness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BC	business continuity
BIA	business impact analysis
CANES	Consolidated Afloat Network and Enterprise Services
CIA	confidentiality, integrity, availability
COOP	continuity of operations
DMZ	demilitarized zone
DODIN	Department of Defense Information Network
DR	disaster recovery
DRaaS	disaster recovery as a service
FAK	fly away kit
HFN	hastily formed network
HP	Hewlett Packard
INFOCON	information condition
IT	information technology
MOC	maritime operations center
MTD	moving target defense
NGEN	Next Generation Enterprise Network
NIST	National Institute of Standards and Measures
NMCI	Navy Marine Corps Intranet
ROI	return on investment
ROK	return on knowledge
RPO	recovery point objective
RTO	recovery time objective
TCO	total cost of ownership
TTP	tactic, techniques, and procedures
VM	virtual machine

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CONTINUITY OF OPERATIONS

Continuity of operations (COOP) is to the Navy what contingency planning is to the National Institute of Standards and Technology (NIST), and what business continuity (BC) is to the private sector: a strategy to maintain operations in the event of a disruption.[1] In this work, "operations" refers to the delivery of network services, including the hosting of applications necessary to conduct regular tasking. "Disruptions" are generally divided into two categories: natural and man-made. Man-made disruptions are further broken down into two categories: accidental and intentional [1]. Within the Navy's Next Generation Enterprise Network,[2] the contingency plans are incorporated into the Information Technology Service Continuity Master Plan (ITSCMP). It is a robust plan to ensure the delivery of services in the event of a natural disaster or accident [2]. This focus of this work is on continuity of operations in the event of an intentional man-made disruption, specifically a network compromise, considering any advantages and opportunities virtualization technology may offer COOP planning.

Continuity of operations is not a new idea. Its military implementation has been influenced by the global political environment, particularly since the beginning of the Cold War, to ensure operations are able to be executed, or risk failing in the defense of the United States and its interests [3]. COOP is, at a fundamental level, simply having a plan to continue in the face of (largely) unplanned events [4]. What is new is the medium in which we are using it—cyberspace. This requires a shift in mindset and priorities. Ensuring delivery of IT services does not necessarily mean a physical relocation of network operators, but it does require prioritizing services for restoration. Aside from transferring a conventional strategy into the context of cyberspace, one of the problems with network operations COOP planning is that it is often thought of as insurance—good

[1] COOP, contingency plans, and, to a lesser extent, business continuity are used interchangeably in this thesis.

[2] Next Generation Enterprise Network is the contract awarded to Hewlett Packard to operate the Navy Marine Corps Internet. This contract is a government owned/contractor operated model.

to have but hopefully not needed. This is a naïve view in an increasingly contested medium with a low barrier to entry [5]. Since a COOP plan is required by National Security Presidential Directive 51 and Homeland Security Presidential Directive 20 [6], this work examines opportunities presented when the cyber environment is tailored toward increased resiliency.

Operationally, the advantages of a COOP plan that includes BC in the event of a compromise may range from augmenting normal operations to military deception opportunities. It also yields benefits to maintenance and training, which will be discussed in Chapter III. For normal operations, contingency plans may be implemented in order to maintain continuity while changing the network posture—also known as network maneuver. This may be to support training, maintenance, or in response to threats, or in order to obfuscate information an adversary may glean from our network traffic.

B. RESILIENCY

Resiliency is applied to many subjects with equally many nuanced and tailored definitions, but the core aspects of resilience are "preparing for, preventing, or otherwise resisting an adverse event" [7]. Resilience is the overall goal of COOP plans, but those plans are only one facet of resiliency. Cyber resilience is more than defending a network against attacks; it is more holistic in that it provides contingencies before, during, and after the disruption. It can be summarized succinctly as follows [8]: "Anticipate and prevent successful attacks on data and networks, and prepare for and operate through cyber degradation and attack."

The characteristics of resilient cyber systems, modeled on resilient physical systems, are the ability to resist disruptive events in the environment, survive impact, recover [9], and adapt to these events [10]. The following is a breakdown of cyber resiliency engineering, and how contingency plans adhere to the principles of resiliency.

1. Cyber Resiliency Engineering

Cyber resiliency engineering is a component of mission assurance engineering, but also the resulting convergence of mission assurance engineering, cybersecurity and resilience engineering [7].

2. Resilience Engineering

Resilience engineering predates cyber, as a domain or a concept. The tenets of resilience are broad enough that they are easily adopted by more specific areas of focus. This is evidenced by Hollnagel, Nemeth and Dekker's cornerstones of resilience—anticipation, monitoring, response, and learning [11]—being mapped to the four goals of cyber resiliency [7]—anticipate, withstand, recover, and evolve.

a. Anticipate

The Anticipate phase involves foreseeing and forestalling disruptions by meeting the following objectives: predict, prevent and prepare for adverse events [7]. The third objective, prepare, is the first layer in which COOP planning applies to resilience.

b. Withstand

The Withstand phase is the ability to "fight through" an adversarial action [7]. The goal of contingency planning and "withstanding" are congruent in that operations must continue. It is during this stage that contingency plans are activated.

c. Recover

Without an adequate COOP plan, the Recovery phase can be protracted and problematic. COOP planning needs to be complete and tested in order to be of significant benefit during this stage. The objectives of recovery are damage assessment, service restoration, and reliability determination [7].

d. Evolve

The Evolve phase is the key to continued relevance regardless of organizational focus. Simply put, the Evolve phase consists of reviewing and revising tactics to prevent

or prepare for changing threats [7]. There are very few static facets of operations, and this true as well for contingency planning. A COOP plan should be regularly reviewed to determine viability against emerging threats and vulnerabilities. It should also consider updated tactics and technologies that may be able achieve the same result with lowered overhead costs. Computer hardware virtualization, or simply virtualization, are technologies that may be able to ensure business continuity is a dynamic process that offers a continuity of operations with less investment in additional physical resources than traditional COOP plans.

C. VIRTUALIZATION

Conceptually, virtualization began as a means of efficiently using resources in order to utilize, as fully as possible, available processing power. Currently, virtualization is still primarily a means to maximize resources as processing power often eclipses application requirements by orders of magnitude. Virtualization is a means to use under-utilized processing capacity to perform tasks in parallel. It allows organizations to maximize the output of their resources at hand with minimal investment in additional physical infrastructure [12].

Retaining current functionality without the addition of physical resources also provides the ancillary benefit of making contingency planning easier [13]. Having less physical infrastructure to account for and secure is ideal from a cost standpoint, but may lead to reduced redundancy, which is anathema to contingency planning.

1. Types of Virtualization

There is an increasing amount of types of virtualization, but the major types are server, application, presentation, network, and storage [14].

a. Server Virtualization

In a conventional network setup, a common practice was to provide one server per service. Virtualizing servers allows multiple servers to be hosted on one physical machine, maximizing that machine's resources, reducing infrastructure cost and footprint [15].

b. Application Virtualization

Application virtualization is where an application is run remotely from the machine on which it is installed [14]. Applications run as if they are installed on the local host, directly interfacing with its native resources, but application virtualization substitutes a portion of the runtime environment an installed application typically uses with a redirection to the virtualized environment the application is actually executed in. There are two main methods to provide application virtualization [16]. The first, and probably most in-line with the moniker "application virtualization," involves the creation of an exclusive run time environment for the application on the machine on which it is installed. The second method is typically referred to as "application streaming" or "application server virtualization." Application services are not performed on the client, rather they are delivered to the client.

c. Presentation Virtualization

With presentation virtualization none of the application's work is done on the host the user is using to access the application. Rather, the user's host is analogous to a repeater that displays an instance of a shared environment [17]. Two of the leading products for presentation virtualization are Citrix XenApp and Microsoft Terminal Services. These services allow many users to utilize applications without having to install the application on their host machine.

d. Network Virtualization

Network virtualization involves deploying logical versions of various layer devices, providing the ability to make multiple virtual networks using the physical resources and IP addresses of one physical network. Again, this is focused on maximizing the use of processing capacity while maintaining or reducing physical resources [18].

e. Storage Virtualization

Storage virtualization uses disparate physical storage devices managed by a virtual storage system to create a single logical storage system [14]. Storage virtualization

is generally divided into two types: block virtualization and file virtualization [16]. Block virtualization is often referred to as a Storage Area Network or as Network attached storage. It is similar in principle to RAID (Redundant Array of Independent Disks) in that there are multiple parts acting in concert, but are recognized as a single device. File virtualization gives the impression that a file may be stored statically on a drive, but in reality the "file" is just a directory tracking where the actual file is stored. An example of this technology is Hadoop Distribution File System (HDFS).

2. Virtualization Security

Since the inception, and rapid adoption, of virtualization technology, virtualized environments have been considered security challenges [12]. This may be because security has largely been a "bolt on" service, not inherently part of the system, and virtualization is focused on maximizing a system's native resources. Although it would seem that the added security features should already protect the hypervisor and virtualized systems [19], this is not the case. However, there are security features inherent to virtualization [19].

Security professionals often cite ease of file sharing, deployment of corrupted hosts, and potential man-in-the-middle vulnerabilities as challenges to operating in a virtual environment [12], [19], [20]. Many of these same sources recommend proper configuration and active management of virtualized resources for mitigating many of security concerns. Notably, the hypervisor is recognized as a potential single point of failure in terms of compromising a virtual network. While potentially vulnerable, the hypervisor is stripped down to provide only the services needed to emulate the physical hardware for virtual machines and, as a result, has a very small attack surface [19], [20].

Inherent security benefits to virtualization include smaller attack surfaces and physical footprints. Virtual machines and networks also largely operate in logical isolation, reducing the attack vectors available to adversary actors. In the event of network compromise a "pristine" version of the network is maintained in addition to snapshots known to be free of malware [17], [21].

D. PROBLEM STATEMENT

Operation Rolling Tide brought into glaring relief deficiencies in the U.S. Navy's plans for operating in a compromised network environment. With the highest level of administrator accounts compromised, and without an appropriate contingency plan from which to enact a timely mitigation strategy, network maneuvers conducted to regain positive control of the Navy Marine Corps Intranet (NMCI) proved difficult and cumbersome [22], [23]. This event illustrated the importance of robust and thorough contingency planning. It also serves an example of how detailed contingency planning for natural disasters and accidental outages does not necessarily translate to contingency plans for operating in an environment under attack.

When contingency planning is conducted with the threat of a successful attack in mind COOP plans may allow normal operations to be conducted in the event of a network intrusion, and may contribute as well to cyber resilience. Cyberspace is unique among the warfighting domains in that is was created by man and dependent on the things of man to function. Like the other domains, however, cyberspace is susceptible to natural forces as well as human action, intentional or otherwise, and it is in our best interest to ensure we are able to conduct operations in times of adversity. As it is implemented at this time, the COOP plan for NGEN is viewed as an insurance policy against outages rather than a key component in mission resilience and mission assurance engineering [2], [24]. This work explores business continuity in a compromised environment, specifically focusing on virtualization and whether it can be leveraged to provide high fidelity command and control (C2) during the recovery phase.

E. RESEARCH QUESTIONS

In order to operate a network during a compromise it is beneficial to have a contingency plan that addresses how mitigation efforts will be coordinated. Plans for a loss of services only, primarily, focus on the availability aspect of the Confidentiality, Integrity, and Availability (CIA) triad, whereas plans to mitigate unauthorized access tend to focus on the Confidentiality and Integrity portions. The following questions guided the research conducted in this work.

1. Is virtualization technology a viable option for COOP in the event of a compromise?

2. In what capacity could virtualization work to our advantage in the stage between detection and mitigation?

3. Will a virtualized environment scale appropriately?

4. What are the costs of adopting virtualization technology?

F. BENEFITS

The results of this work will determine if virtualization is an appropriate technology for use in COOP planning, particularly focused on leveraging its benefits to develop and deploy tailored spaces for maintaining C2 in the event of a compromise. Additional benefits may be realized by leveraging virtualization technology in COOP plans to augment operational exercises, and increased readiness at sea as CANES is deployed to the Fleet.

G. METHODS

This work reviews published literature on BC, disaster recovery (DR), virtualization technology, virtualization products, and virtualization security tactics, and weighs them against current NGEN COOP plans and readily available options for use in the event of a network compromise.

H. LIMITATIONS

This work is conceptual in nature, meant to explore the viability of the use of virtualization technology in NGEN as a response to adversarial action. However, before that could be a consideration, it was necessary to determine what network compromise DR might look like. While virtualization products are being sold in the private sector for disaster recovery as a service (DRaaS), they, like NGEN's current COOP plans, are geared toward unforeseen outages rather than a persistent, unauthorized presence on the network. The bulk of this work deals with the idea of how continuing operations during a compromise may be possible while still maintaining a degree of network C2. While it provides tactics that may be employed to accomplish this, a technical model determining the means by which these tactics may be carried out is left to future work.

I. THESIS ORGANIZATION

1. Chapter II: Continuity of Operation Strategies

Chapter II contains an overview of disasters, differentiating the needs of BC in unplanned outages due to natural disasters or man-made accidents and disasters due to intentional, adversarial action. It reviews options available and readily adoptable technology available to DODIN for use in a compromise. Finally, it looks at virtualization technology and its applicability to COOP in the event of a compromise by analyzing the manner in which it may contribute to defensive cyber operations (DCO)

2. Chapter III Costs of Adopting Virtualization Technology

Since this work examines the benefits of virtualization to COOP during a compromise, the cost analysis is not focused on where the technology will save the Navy money. A particular focus will be on manpower, training, and maintenance costs, as those areas are likely to be the largest recurring costs, in light of the fact that the use of virtualization technology, toward the goal of contingency planning, is not intended to replace existing infrastructure, or streamline normally offered services.

3. Chapter IV: Results

The final chapter provides the results of the research, and a recommendation on whether virtualization is a viable, and economically sound, strategy for use in the event of a compromise of NMCI. It also outlines future work exploring moving target defense as a viable strategy for a virtualized tailored space.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CONTINUITY OF OPERATIONS STRATEGIES

A. NATURAL DISASTER VERSUS ADVERSARIAL ACTION

A disaster is a natural or manmade event that has a negative effect on the operating environment and infrastructure [1]. Although contingency planning traditionally focuses heavily on withstanding natural disasters, with the steady increase in cyber-attacks, maintaining operations in the event of adversarial action is becoming a major concern among cybersecurity professionals in the private sector [5], [25]. The Chief of Naval Operations has included the development of cyber defense in his Sailing Directions [26]. Since many organizations are increasing their online footprints to keep pace with competition, it seems logical to anticipate that an attack will, eventually, be successful. Accounting for the increased threat of a cyber-attack by investing in cybersecurity has transitioned from a competitive advantage to a cost of doing business [27]. Adding DR and BC considerations into security plans adds a layer to the defense-in-depth concept, perhaps making "continuity in depth" a more appropriate term.

Proper implementation of a COOP plan must begin with designing the proper COOP plan for the organization. In organizations that are combative in nature, such as the Navy, contingency plans must take adversarial action, as well as environmental factors, into account. Options for BC in the private sector are vast, seemingly limited solely by the amount of money an organization is willing to spend. Interestingly, though, when it comes to contingency planning, disasters caused by adversaries are largely ignored by vendors offering DRaaS. The primary strategy for cyber-attacks is to maintain a strong defense. This is accomplished by including defense as the IT department's responsibility, or, increasingly, contracting with a vendor that specializes in cybersecurity. As for defense being a single layer of "continuity in depth," a competent defense fulfills the Anticipate phase of resiliency, but when an attack is successful, the Withstand phase transitions from solely relying on a strong and layered defense to network defense and the implementation of COOP plans in order to "fight through" the compromise.

1. Planning for Intentional Disasters

There are some factors in play for network administrators in the decision as to how much to invest in COOP planning. Many of these factors are considered during business impact analysis. Business impact analyses anticipate an organization's losses during a disaster, and serve as a useful tool in the cost/benefit analysis of various BC and DR options [28]. Other factors that may influence the cost benefit analysis are size, precedence, and sovereignty of an organization. As a factor size is not measured merely by the cost of repairing or replacing equipment, but also by considering whether the network is large enough to be maneuvered in such a manner that services can continue during the Withstand and Recovery phases. The question of precedence is less network-centric, but how skillful the organization's cyber security personnel are, and how much an organization is willing to invest in adhering to or challenging applicable laws. Sovereignty, as it is traditionally—and currently—used, is the possession of the legal status of a state. With that status, comes the potential for loss beyond monetary damages in the event of a disaster. For a state, loss can manifest as a loss of faith in the government to protect itself and its citizens, as well as potentially reduced international prestige [22]. Sovereign nations have more options in terms of defense and continuity. Most notable among these options is the ability to fight back [29]. All losses and capabilities must be taken into account when conducting a BIA in order to determine the best COOP option.

B. DODIN AVAILABLE OPTIONS

NGEN's COOP strategy is well defined for natural disasters and other environmental conditions [2]. In the event of intentional network compromises, it provides little guidance, and network administrators must generate a plan on the fly to regain control. From the time of intrusion discovery to successful mitigation, all operations must be conducted in a compromised environment. This is a reactive posture that runs counter to the Anticipate phase of resilience [7], and potentially puts unnecessary stress on the C2 of network operations. At this time, there are few options available that allow the Navy to adopt a proactive posture.

The subsequent sections list options available for utilization within the framework of a COOP plan. Some of these options (Information Operations Condition, Rerouting) are part of the Navy's standard operating procedure [30], [2]. Others (Isolation, Alternate Sites-Hot Site) are included in current COOP plans [2]. The remaining options are commercially available, but not included explicitly in the NGEN contract.

1. Information Operations Condition

Information Operations Condition (INFOCON) is a framework allowing commanders to adopt a network posture appropriate to the operating environment. Currently, it is the best tool available for maintaining positive command and control of their networks, in that it allows for some anticipation of the level of adversity in the environment. "The INFOCON system provides commanders the authority, discretion and accountability to prepare their organization's network and information systems at any level they deem appropriate for the current and anticipated environment" [30].

2. Rerouting/Backhauling

Currently NGEN's primary BC strategy is to reroute, or "backhaul," services from the station where the services are leased to another telecommunication station [2]. This strategy works particularly well in the event of disasters that provide some lead-time, such as hurricanes, and it provides flexibility for unpredictable disasters, such as earthquakes, but places increased stress on existing infrastructure [4].

3. Isolation

Another option available to commanders is removing a unit from the DODIN [24]. Removing a unit from an assault is a viable tactic for withstanding the assault, though that unit's contributions to the overall operation will likely be significantly reduced. This action can be initiated at the unit level, but is typically carried out by direction of Commander, Tenth Fleet. This can be advantageous in regard to severing an adversary's line of communication, but, depending on the autonomy of the disconnected unit, this tactic may hinder operations or operational objectives.

4. Alternate Sites

A popular strategy for withstanding a network-impacting event is maintaining an alternate site. This may be less germane to incidents of cyber-attack in terms of recovery point objective (RPO) and recovery time objective (RTO) for NGEN as a whole, as the objective for recovery would likely be removing unauthorized presence and code as soon as possible, in the event of a compromise. Alternate sites can provide a secure physical environment for the coordination of routine operations as well as determining network maneuver in defense of our cyber domain.

Many Navy organizations that heavily rely on network connectivity have, as part of their COOP plan, an alternate site from which to perform their missions. Often this consists of sharing space at another organization's facilities. NGEN is responsible for network connectivity to at least one hot site [2]. Though it may be arduous to establish connectivity at these sites due to contractual constraints, there are commercially available sites specifically configured for business continuity and disaster recovery [4].

a. Hot Site

A hot site is a space, typically manned, prepared to assume the normal operations of an organization upon the implementation of a COOP plan [4]. These sites need little to no configuration changes once activated, and network data is frequently replicated to the hot site systems. As stated above, NGEN provides network services to at least one dedicated hot site. Organizations that agree to share space and resources in the event of COOP plan implementation can be considered hot or warm sites, depending on the availability of resources at the COOP location.

b. Warm Site

Warm sites are maintained in a ready status, but may need some degree of augmentation to the existing network infrastructure prior to assuming operations [4]. Data replication is not as frequent as it is with a hot site, and the time required to fully implement a COOP plan is somewhat slower than a hot site [4].

c. Cold Site

A cold site is just a space capable of supporting operations [4]. Basic infrastructure is provided, but all equipment necessary to provide network services is to be installed by the contracting organization upon implementation of the COOP plan.

d. Mobile Site

Mobile sites contain specific, portable equipment necessary to provide network services [4]. HP provides this capability in the form of fly away kits (FAK), most notably in the form of the Deployable Site Transport Boundary [31].

e. Mirrored Site

Mirrored sites are the most robust option for backup sites [4]. A mirrored site varies from a hot site in that it is an identical network that is updated in real time vice a network that provides the same capabilities updated frequently. Typically these sites are not contracted out; they are operated and maintained by the organization.

f. Portable Network Infrastructure

Portable network infrastructure is similar to a FAK in concept, but rather than providing the services required to access NMCI, it is a self-contained network infrastructure. It contains the necessary power, communications and servers required to function as a network. Like the "Emergency Operations Center in a box" from [32], this technology would be best utilized by a site experiencing a degraded capability to deliver services. Whether this degradation affects service delivery due to unintentional disaster, or possibly due to kinetic action, a portable network infrastructure may provide the processing capacity needed to implement a tailored space to assist in mitigation efforts [33].

5. Consolidated Afloat Networks and Enterprise Services

Consolidated Afloat Networks and Enterprise Services (CANES) is not a component of current COOP strategies; it is a system to efficiently deliver IT services to the Fleet. It is a good example of the Evolve phase of resilience in that it was developed

to meet the networking needs of afloat units, but the design accounts for the adoption of virtualization technology in future upgrades to the system [34], [35]. The advantage of CANES having been designed with virtualization technology in mind is the opportunity for afloat network training to overlap with that of shore networks, should NGEN adopt virtualization, likely resulting in an increased degree of readiness in the cyber domain.

C. VIRTUALIZATION AND COOP

Many have touted the virtues of virtualization, from added capabilities to reduced server sprawl. For small organizations, the argument for adopting virtualization technology is to not waste money on infrastructure that can be virtualized. For large organizations, the argument for adopting virtualization technology is to cut costs by shedding some infrastructure. For the federal government, virtualization may help relieve the unsustainable growth of its data centers, and support the Federal Data Center Consolidation Initiative [36]. The assumed benefits of virtualization are that costs will be lower, the footprint will be smaller, and current infrastructure will be utilized more efficiently [37], [38]. Since an investment in DR of BC may never realize a return, it is understandable that virtualization technology, offering the same benefits at a lower price, presents an attractive option.

The same qualities that make virtualization an attractive option for DR and BC can also provide benefits to normal operations. Potentially getting more productivity from the same, or less, infrastructure typically leads to reduced costs of maintaining that infrastructure, leading to increased overhead [37]. Its flexibility lends itself well to business continuity [13]. How can virtualization be advantageous in withstanding and recovering from a network compromise? To draw an analogy from the physical domain of warfare: adversarial action is conducted in the contested space (i.e., the front lines), C2, planning, and strategy development typically occur in safer areas, somewhat removed from the threat of violence. If the network is considered the front lines of the conflict, where is the remote location from which the battle is orchestrated? SIPRnet is available to use in such a capacity, but virtualization leveraged in a hastily formed network (HFN) concept [32] could provide such an environment with greater penetration than SIPRnet.

Creating a virtualized environment as a shared conversation space allows for the rapid connection of personnel from various communities to plan and execute actions to fulfill an urgent mission [32], [39]. After an attack has been identified and classified, the organizations responsible for conducting defensive cyber operations will determine who the stakeholders will be and what their duties are. Those commands will appoint personnel to fulfill these assigned duties and meet promulgated operational objectives. Virtualization technology can be used to create an uncontested, collaborative environment from which DCO is coordinated. These tailored spaces are created for the purpose of maintaining C2 of mitigation efforts. Determining whether C2 is of high or low fidelity, for the purposes of this work, is based upon whether operations are being conducted in a compromised environment (low fidelity), or if it in a space in which a reasonable degree of security from adversarial action can be assured (high fidelity). The concept of C2 COOP is founded on the basis that mitigation planning and coordination efforts are obscured from the intruder.

There are difficulties in planning a COOP strategy that the adoption of virtualization does not alleviate. The average time to detect a network intrusion is two hundred and twenty-nine days, roughly seven-and-a-half months [40]. It is likely that in that time malware has migrated into the virtual environment, and current system snapshots contain the offending code. This introduces storage concerns (depending on how long snapshots and other backups are kept for), and time spent finding a "clean" snapshot, inevitably increasing the RTO. Additionally, there is a cost in managing the virtual environment [41] that makes virtualization an infeasible option for adoption as an NGEN wide COOP plan. While the advantages of virtualization do not directly address these issues, it may prove useful to the coordination of mitigation efforts in an environment that does not negatively affect routine operations. This in effect "fast tracks" the preparation of the uncontested space from which the HFN will plan and implement the overall operation.

In order for C2 COOP to be a viable option, it must provide benefits making its employment worthy for consideration. Ideally, C2 COOP will enable the following:

1. Provide a secure environment from which operations intending to regain control of a contested network can be planned and conducted.

2. Scale appropriately in that implementation of a contingency plan relying heavily on additional networking resources does not add undue hardship on system administrators already mired in conflict nor be so contractually cumbersome as to adversely affect the RTO.

3. Provide some tactical advantage, either in rebuffing the adversary, limiting his movement throughout the network, or contributing to his attribution.

INFOCON, while ideally anticipatory in nature, can also be adjusted to be a reactive measure for DODIN, including NGEN, in an effort to safeguard the confidentiality aspect of the CIA triad [30]. This serves more to dictate how to conduct operations in a contested environment than to ensure continuity of operations, and therefore is not a reasonable option for C2 COOP. NGEN's current COOP options, backhauling services and maintaining hot/warm sites, focus on availability. In addition, the alternate sites may suffer from the same network vulnerabilities as the primary sites, therefore may not contribute to the security of a C2 environment. Furthermore, any additional network resources must be procured and connected to the network. Both of these processes can be time consuming. Commercially available alternate sites, like NGEN's alternate sites, focus primarily on availability. They can be costly to maintain and outfit to the needs of the Navy. While virtualization technology may have a higher initial investment than a number of the options listed here, and incur the additional requirement of training (these aspects will be discussed in Ch. III), virtual environments may be tailored to more acutely address the confidentiality and integrity facets of C2 COOP. The subsequent sections will explore the benefits virtualization may provide to C2 COOP.

D. VIRTUALIZATION TACTICS AND OPPORTUNITIES

The primary goal of virtualization in the event of adversarial action is to create uncontested terrain from which C2 of defensive cyber operations can be established. While the concept of tailoring a space for the purposes of C2 was inspired by the tailored trustworthy space proposal [42], that proposal is likely too nebulous for the inherently temporary nature of COOP [4] Once the operational objectives have been determined,

virtualization can also be leveraged in a defensive capacity to slow the adversary's advance through the network, analyze his tactics, techniques and procedures (TTPs), and potentially contribute to attribution efforts.

1. Virtual Maritime Operations Center

A virtual maritime operations center (MOC) can serve two purposes: create uncontested space from which to plan DCO (for the major stakeholders of DCO), and create uncontested space from which Fleet MOCs can plan operations in the physical domain.. Should a cyber effect against naval C2 be part of a multi-domain operation, a low RTO is critical to maintaining positive C2. If the MOC's services have a suitable level of redundancy, in terms of virtualized services and infrastructure, the MOC may be able to execute a timely failover to a virtualized environment.

Once detected, and malware identified, a virtualized environment can be created, specifically tailored to the needs of the organizations actively combatting the intrusion. The flexibility of virtualization offers an additional benefit in that other tailored spaces can be deployed to act as ad hoc forensic environment in which the rigors of mitigation can be determined. In effect, setting up these virtual spaces not only support C2 of mitigation efforts, but also provide an opportunity to test the initial mitigation strategy and measure its effectiveness with minimal additional disruption to ongoing operations.

2. Virtual Honeypot

Adopting virtualization technology may prove beneficial to C2 COOP, but the flexibility of virtualization technology may also allow for C2 benefits not necessarily directly tied to COOP. Disrupting the adversaries ability to navigate the network likely enhances the defender's control aspect of C2. Virtual honeypots offer many of the same advantages of their physical counterparts but require less infrastructure, therefore they are less expensive to deploy, and are scalable, and easy to maintain [43]. While the deployment of honeypots in an enterprise network is a prudent security practice, the flexibility offered by virtual honeypots provides a number of advantages in affecting the adversary's movement through the network, in intelligence gathering and possibly breaking the kill chain [44].

a. Obfuscate

Honeypots, as they are normally employed, provide value from the monitoring and analysis of unauthorized access[3] [45]. As previously mentioned, the average time between network breach and detection is over seven months, and it is reasonable to assume that in this time the adversary will have developed at least a working knowledge of the network topology. Adding virtual honeypots as a reactive measure may help to obfuscate network characteristics [46]. Such obfuscation may interfere with the adversary's action on objective possibly breaking the kill chain at that level [44]. Employment of virtual honeypots may serve to obfuscate actions taken in support of mitigation operations, potentially prolonging the lifespan of our network defense tactics.

b. Delay

Depending on the configuration of the deployed honeypots, an adversary may get "bogged down" attempting to access these seemingly soft targets. Tarpitting the honeypots causes an adversary to spend time evaluating them, slowing his progress through the network [43], [47]. While slowing the rate of infection, tarpitting may prevent further data exfiltration and allows for another opportunity to break the kill chain.

c. Analyze

In the time between compromise detection and RTO, virtual honeypots can be deployed with the resultant attempts to gain access being monitored and analyzed for actionable intelligence. This may provide an opportunity to determine the TTPs used to move through the network and the variety or varieties of malware that have been infiltrated. Depending on the handling of the collected data, and operational requirements, the information collected may not be suitable to present as evidence in a court of law [48], it may be suitable to base operational planning on.

An alternative to a full, virtualized honeypot or honeynet is the deployment of Nepenthes for the purpose of collecting, analyzing and identifying malware [43].

[3] As honeypots provide no services and store no data to support normal operations, all access is considered unauthorized.

Nepenthes are advantageous because the principle they operate on prevents infection. Instead of having a sacrificial machine, virtual or physical, waiting to be compromised, Nepenthes emulate vulnerable services without running the exploitable service, essentially acting as bait. Depending on the modules employed, nepenthes can even sniff traffic on specified ports.

d. Attribute

Analysis of the honeypot traffic can reveal TTPs that may help to attribute the compromise. While attribution is difficult to prove beyond the shadow of a doubt, it is critical for maintaining situational awareness of threat vectors and the capabilities of potential adversaries [49].

E. TACTICS FOR SECURING VIRTUALIZED ENVIRONMENTS DEPLOYED IN THE EVENT OF A COMPROMISE

1. Virtual DMZ

Furthering the effort to create, and secure, uncontested space, virtualized demilitarized zones (DMZs) can be deployed to offer an additional layer of defense between the contested network and a tailored space without a significant change to the DMZ topology [50]. Virtualized DMZs can be positioned between the compromised network and C2 network, but can also be used to add layers of defense to identified high value targets such as cross-domain solutions between networks of different classification levels.

2. Moving Target Defense

Depending on the urgency of the operation, and the activity level of the adversary, additional tactics may need to be utilized to ensure the virtualized C2 environment remains free of the adversary's influence. Combining VM triage [51] with the concept of moving target defense (MTD) will likely prevent compromise or, in the event of successful penetration, ensure that any compromise lacks persistence.

MTD seeks to shift the asymmetric advantage enjoyed by attackers to the defenders. It does this by combining proactive approaches to configuration management

to reduce attack surfaces and the principles of resiliency in order to secure computing environments [52]. The primary MTD tactic applicable to C2 COOP is the moving attack surface (MAS).

Standing up a virtualized network will introduce new attack surfaces. The moving MAS concept sees those attack surfaces deployed unpredictably and dynamically [53]. This is accomplished by having virtual servers revert to a pristine state randomly or upon indications of compromise. Upon reversion, the VS will occupy a different IP address in the network. MAS does not necessarily reduce the overall size of the attack surface, but it leverages the element of uncertainty to the defender's advantage by reducing the adversary's ability to consistently connect with the same virtual server. VM triage [51] and products like VMotion[4] [54], which enables live migration, are tools with which this tactic could be used.

[4] VMotion by VMWare is a product that provides live migration of virtual machines. Live migration is crucial to employing a MAS tactic in order for it to be transparent to the end user.

III. COSTS OF ADOPTING VIRTUALIZATION TECHNOLOGY

A. COSTS

As the costs for network operation are included in the contract upon award, it is difficult to make a service -to -service comparison of existing COOP plans and a COOP plan utilizing virtualization. Actions are either within or outside the scope of the contract, and handled appropriately. In this case, the use of virtualization technology is adding a capability rather than replacing one, so adopting virtualization technology will undoubtedly increase costs for the Navy, at least in terms of initial investment costs [55]. The total cost of ownership (TCO) for a modest virtual network, with the services of an enterprise level network, is approximately $3.3 million [56]. The operating costs would be less than that of a similar physical network [55], [57], and those expenses may be reconciled with the benefit of an overall increase in readiness. While the costs of utilizing virtualization technology will need to be included in a future contract, the Navy will incur increased cost in the form of training, facilities, and utilities.

Since any return on investment is not likely to manifest itself in quantifiable amounts of money, this chapter focuses on identifying areas where costs will be incurred, as well as return on investment (ROI) in the form of a return on knowledge (ROK). To begin the process some assumptions are made about the capabilities required to deploy a tailored space for the purpose of withstanding a cyber-attack, the personnel—and their skill level—required for the tailored spaces to function effectively, and the organizations that will likely deploy tailored spaces as an element of their COOP plans.

The following subsections list some of the expectations regarding the deployment of tailored C2 spaces. The three aspects discussed are the capabilities expected to be native to a tailored C2 space, the types of personnel expected to operate in these spaces, and the commands most likely to deploy virtual environments in response to a network compromise.

1. Capabilities

Two primary capabilities are necessary for effectively leveraging a tailored C2 space in support of network maneuver: collaboration and network modeling [58]. These capabilities are commercially available and are developed by mature companies. Cisco offers collaboration tailored to virtual environments as part of Business Edition 6000 for a cost of $9,400 [59], [60]. Riverbed Modeler[5] offers high-fidelity network modeling through partners for $46,100 [61], [62].

2. Personnel

Three categories of personnel have been identified as the primary clients of a tailored C2 space: virtualization users, managers of virtualized networks, and network modelers.

a. Users

This is the broadest category, and includes anybody working in the virtualized environment. There is a low barrier to entry as most skills will transfer from the primary network environment, but training on the unique aspects of virtual environments will be required to operate efficiently. Training the end user in the routine tasks common to a virtualized environment also serves to reduce the strain on the virtual network managers.

b. Virtual Network Managers

Analogous to their traditional network counterparts, the virtual network managers assume the responsibility of containing VM sprawl as well as deploying and connecting the more involved aspects of the network, such as servers and virtual infrastructure. Security concerns may arise if managers are not given specific training in virtual network operations [12].

[5] Riverbed bought out OPNET, and currently offers the OPNET Modeler Suite as Riverbed Modeler.

c. Network Modeler

Network modelers will have similar training to that of virtual network managers, but they require operational knowledge as well. In order to determine the evaluate potential courses of action, modelers will need to simulate the compromised environment, or a portion of it. This will allow them to determine the options that most effectively and efficiently combat intrusions.

3. Organizations

Virtualization offers the opportunity for deploying virtual environments nearly anywhere, but only a few primary organizations are likely to use them in response to a compromise. These organizations consist of Tenth Fleet, Naval Network Warfare Command, Navy Cyber Defense Operations Command, Navy Information Operations Command Norfolk, and Naval Computer and Telecommunications Area Master Stations Atlantic and Pacific, as well as their subordinate stations located in fleet concentration areas.

B. AREAS OF INCURRED COST

The following are the primary areas in which the Navy will spend in order to develop the infrastructure necessary to host tailored spaces. Initially, largest expenditure will be the upfront costs of purchasing and installing the required hardware. Recurring costs, in operating expenses, for a virtual network supporting one thousand VMs with an enterprise operations package are projected to be $343,500 per year [56], totaling approximately $1.7 million over a five year contract.[6] These costs per year are based on a projected utility cost of ($43,700 at $.1 per kilowatt hour), data center operations ($5,200), software and server support ($265,000), and administrative costs ($29,500) [56].

[6] The projected operating cost of $343,500 per year is likely a high estimate. Given this virtual environment is not intended to be used as a production network, costs will likely be lower; dependent on how frequently the network is utilized, and in what state the servers are kept in (hot, warm, cold).

1. Up-Front Costs

The initial costs of an investment in virtualization technology are manifested in hardware, software, labor, and transport [55]. Hardware consists of the physical virtual server and related infrastructure. Software includes software packages and licenses required to operate proprietary programs. Labor covers the cost of contractors preparing the physical space—and man-hours of military personnel assisting—as well as installation of the servers and their logical set up. Transport is the cost associated with contracting with the Defense Information Systems Agency (DISA) to connect the virtual servers to the DODIN.

2. Facilities and Utilities

Due to the relatively small footprint required by virtual technology, it is unlikely that construction of a new facility will be required. It may be necessary to prepare a portion of an existing facility, depending on the original purpose of the space chosen to house the servers, to potentially include improved access to power, backup power, LAN connections, additional environmental controls, raised floors, wiring harnesses, and bulkhead penetration [63]. These preparations generally cost between $600 and $900 per square foot [64].

3. Training

It has been noted that one of the weaknesses of virtual networks is the ease with which they can grow beyond the control of the administrator [41]. Herein, we find a cost of using virtualization technology that is likely going to be higher than private sector use, due to the itinerant nature of naval personnel. Developing tailored C2 spaces using virtualization, will require an increase in training expenses. However, since virtualization

will be adopted in the Fleet through the deployment of CANES [35], the cost of independent instruction of the Navy's information system technicians (ITs), or even a possible new "C" school will increase readiness not only ashore, but at sea as well.

C. RETURN ON INVESTMENT

As mentioned previously, a contingency plan for fighting through a network compromise is good to have, but hopefully never needed. With that said, contingency plans do not have to be an investment with no returns, though the returns may be difficult or impossible to monetize. The main aspect in which a virtualized C2 COOP plan will yield a return is in readiness. Having a COOP plan that is designed to be implemented in parallel with routine operations allows for the cyber aspect of Fleet exercises to be included rather than being relegated to table-top walkthroughs. Increased readiness paired with increased resilience primes our forces to respond effectively in the case of a planned attack in the cyber domain.

D. RETURN ON KNOWLEDGE

In order to quantify ROI, Housel and Bell's knowledge value added methodology [65] was used to correlate investment to an increase in readiness. The three core areas identified were evaluated using metrics described below to determine a percentage of ROK.

Table 1. Knowledge Value Added Assessment

Core Areas	Users	Virtual Network Administrator	Network Modeling	Totals
Difficulty	1	2	3	
Relative Learning Time (Total Time=36 Months)	2	6	7	15
Number of Personnel	260	26	14	300
Percentage of Automation	80%	40%	50%	
Amount –of Knowledge Embedded in Automation	416	62.4	49	527.4
Total Amount of Knowledge	936	218.4	147	1301.4
Percentage of Knowledge Allocation	71.9%	16.8%	11.3%	100.0%
Annual Expenditures (Millions)	.73	0.17	0.12	1.02
Readiness	4	4	4	
Return on Knowledge (percent)	5.5	23.5	35.3	

Table 1. Housel and Bell's KVA assessment methodology applied to contingency planning.

a. Core Areas

The core areas parallel the personnel roles in a tailored C2 space: Users, virtual network managers, and network modelers.

b. Difficulty

Ranked 1 through 3, the core areas were judged by the level of training required and whether the duties were solely technical, or involved operational planning aspects as well.

c. Relative Learning Time

Learning time was determined by determining which roles rely primarily on on-the-job-training (OJT) and which required formal training in order to perform competently. Also considered was analogous training already offered by the Navy, including any prerequisites required [66]. The total time is based off the shore rotation tour length of Navy Information System Technicians [67].

d. Number of Personnel

The numbers selected for this variable are assumptions based largely on organization size, responsibility, and placement in the operational chain of command. Conceptually, for the purpose of this assessment, it was assumed that only the personnel assigned to combatting a network compromise, at each invested command, would need access to the tailored space. This allows the tailored space to remain relatively small and streamlined, therefore reducing the workload on the managers. It is also in the interest of security that personnel not directly involved in coordinating the mitigation should not have access to the tailored space.

e. Percentage of Automation

This percentage is assigned based, largely, on how user-friendly the programs and services used are, essentially reducing time required to train a user [65]. For example, cloning a virtual machine is fairly easy, even for a novice user, so the knowledge contained in automation is given eighty percent for the system. The virtual network

managers, on the other hand, need significantly more training to do their job effectively, even with the guidance native to the system used, hence forty percent is assigned to automation.

f. Amount of Knowledge Embedded in Automation

This value is determined by multiplying the relative learning time (RLT) by the number of personnel (NOP) and the percentage of automation (POA). This combines the learning time of all personnel with automation providing a quantity that can be used to calculate the total amount of knowledge in the core area.

$$RLT \times NOP \times POA = AKEA$$

g. Total Amount of Knowledge

This value is determined by multiplying the RLT by the NOP and adding the amount of knowledge embedded in automation (AKEA). Determining the total amount of knowledge for each core area provides the information required to determine the percent of knowledge allocation per core area.

$$RLT \times NOP + AKEA = TAK$$

h. Percentage of Knowledge Allocation

This value is determined by dividing the total amount of knowledge (TAK) for an individual core area by the sum of TAK over all the core areas, and multiplying the resulting value by 100 to yield a percentage. Calculating the percentage of knowledge allocation (PAK) allows for determining how much of the annual expenditures are dedicated to each core area.

$$(Core\ Area\ TAK \div Total\ TAK) \times 100\% = PKA$$

i. Annual Expense

This value was determined by dividing the sum of the TCO, collaboration and modeling software costs and dividing that by a five-year contract length. That value was added to the estimated yearly operating costs to yield the total annual expense. The total

annual expense was multiplied by the PAK to produce the annual expense (AE) for an individual core area. In the context of the enterprise as a whole, the NGEN contract award price [68] is divided by the length of the contract (five years), and that value is multiplied by the percentage of Knowledge Allocation (PKA). Determining the annual amount of money being spent on each core area provides half of the equation for determining the return on knowledge for a core area.

$$\Big(\big((TCO + software\ cost) \div 5\big) + operating\ costs\Big) \times PKA = AE$$

j. Readiness

In order to find a substitute for the annual revenue column of Housel and Bell's KVA methodology, readiness, measured in participation in exercises, Fleet or internal, was used as a surrogate for revenue. Quarterly exercises were used as an ideal case, and semiannual exercises as a more realistic expectation.

k. Return on Knowledge

This value is determined by dividing annual expense (AE) by readiness (R). Calculating the ROK within the context of contingency planning, where the AE consists of the yearly operating costs added to the TCO (including collaboration and modeling software) divided by the length of the contract. In this scenario, considering optimal exercise participation, the ROK is 5.5 percent for users, nearly 23.5 percent for virtual network managers, and 35.3 percent for network modelers. Considering the more realistic scenario of two training events per year, ROK is halved to 2.8, 11.8, and 17.7 percent respectively. It should be noted that, when computing ROK in the context of the NGEN contract as a whole, ROK peaks at .1 percent for network modelers with the remaining core areas dropping off precipitously.

$$R \div AE = ROK$$

E. DRAWBACKS TO IMPLEMENTING VIRTUALIZATION INTO COOP PLANS

There are numerous reasons to invest in a well-crafted contingency plan, including the likelihood of increased adversarial activity [40], best practices [4], and presidential directives [69], but there are some disadvantages. As an added service, there is an increase in cost that will not likely be mitigated by gains, tangible or intangible, at least in the near term. The level of expertise of system administrators will likely atrophy more quickly until virtualization becomes more common in the Fleet after CANES is deployed. In order to reap any return on investment,C2 COOP should be practiced often as part of Fleet or internal exercises. Also, all defensive layers, in the tailored space and the physical network, need to be implemented as competently as possible and continually kept in complimentary configurations, increasing maintenance efforts. COOP plans focusing on C2 must also be reviewed an updated to maintain situational awareness with current threat vectors. This review is already written into the NGEN contract [2].

IV. CONCLUSION

A. RESULTS

This work examined the concept of continuity of operations and resilience in the face of a network compromise. Specifically it researched the potential benefits of utilizing virtualization technology to establish a tailored space for the purpose of maintaining C2 during mitigation efforts. The following subsections are the results of the research as applicable to the research questions this work was based on.

Virtualization technology is a versatile and relatively inexpensive means to augment NGEN operations. With the implementation of CANES onboard Navy ships it appears that virtualization has a significant role to play in naval networks in the not too distant future. Using virtualization technology to develop and deploy tailored C2 spaces can be a valuable tactic to keep the adversary out of the leadership's OODA loop[7] when control of the primary network is contested.

Savings is a benefit of infrastructure virtualization. From the analysis conducted here the use of virtualization to provide C2 COOP capabilities would cost more, although the cost of developing virtualized C2 environments is only approximately one tenth of one percent of the NGEN contract award. Further, yearly operating expenses are estimated to be approximately $344,000, or .01 percent of the total contract. Continuing costs must also include training costs. Readiness will be the primary positive return on investment resulting from the pursuit of virtualization technology for C2 COOP. To quantify the ROI, the knowledge value added assessment performed showed positive, if somewhat modest, increases in readiness.

1. Is Virtualization Technology a Viable Option for COOP in the Event of a Compromise?

The answer to this is a qualified yes. The technology and tactics are available to ensure that a virtualized environment can be used to create tailored spaces in an effort to

[7] The OODA loop is a process based on these principles: observe, orient, decide and act.

provide reasonably widely accessible, high fidelity C2 of mitigation efforts addressing a network intrusion. In terms of reducing the RPO to less than six months, which was the duration of Operation Rolling Tide [70], virtualization technology appears to be an attractive option.

2. In what Capacity could Virtualization Work to an Advantage in the Stage between Detection and Mitigation?

In addition to providing the ability to deploy tailored C2 spaces, virtualization technology may benefit the "control" aspect of C2. If it is determined to be advantageous, or necessary, virtual honeypots, Nepenthes [43], and virtual DMZs [50] can be deployed to potentially disrupt adversarial activity within the network.

3. Will a Virtualized Environment Scale Appropriately?

One of the selling points of virtualization technology is its inherent scalability. In terms of appropriate scalability, a primary requirement is the ability to add resources without unduly increasing cost, stress on the infrastructure, and complexity for the system administrator. Considering those factors, virtualizing an enterprise network such as NMCI is infeasible from a system administration standpoint. On the other hand, with proper network management, virtualization technology can scale to the needs of a tailored C2 space without significantly adding to man-power costs.

4. What Are the Costs of Adopting Virtualization Technology?

Using virtualization technology as part of a C2 COOP plan will not save the Navy money at this time, but the cost of operating and maintaining the infrastructure necessary is significantly less than that of physical infrastructure leveraged for the same purpose [55]. While the costs do not appear to be prohibitive, given the financial climate of the last few years, it may be necessary to postpone the addition of a C2 COOP solution until next contract for enterprise network services. Until then, C2 COOP will not be supported.

B. FUTURE WORK

1. Technical Model of Virtualized Tailored Space Using Moving Target Defense

The next step in determining the feasibility of using virtualization technology as part of a C2 COOP plan is to develop a virtual network that meets the criteria set forth in [42] utilizing moving target defense tactics. The aim of this should be twofold: determining if the virtualized network can sustain operations using moving target defense tactics, and the most beneficial configuration of this tailored space to respond to a network compromise. This knowledge would help determine what must be considered for inclusion in contract proposals if C2 COOP were to be adopted.

2. Tailored Tactical Space Using Virtual Honeypots

A topic worthy of future exploration is how to best leverage virtual honeypots in order to wrest advantage from the adversary. Is it worth developing a tailored tactical space for use in concert with a tailored C2 space? Virtualization technology is flexible, perhaps flexible enough to tailor a space in which we could "meet" the adversary using honeypots and Nepenthes. What United States Code title authorities, if any, apply to this potentially more active defensive posture? If virtualization technology is leveraged to create terrain for the purpose of interacting with an adversary, that terrain would likely need some definition, and applicable U.S. Code authorities must be identified to determine the scope of actions legally available for employment.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] EC-Council, *Disaster Recovery*, Clifton Park, NY: EC-Council Press, 2011.

[2] H. P. E. Services, *IT Service Continuity Master Plan*, Herndon, VA; H. P. E. Services, 2015.

[3] RAND National Defense Research Institute, *Ensuring Military Capability: Continuity of Operations*, Arlington, VA: The RAND Corporation, 2001.

[4] National Institute of Standards and Technology, *Contingency Planning Guide for Information Technology Systems*, U.S. Government Printing Office, Washington D.C., 2002.

[5] *Internet security threat report* (2014 Apr), Symantec, [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[6] *FEMA* (4 May 2007), Department of Homeland Security [Online]. Available: http://www.fema.gov/guidance-directives

[7] D. J. Bodeau and R. Graubart, *Cyber Resiliency Engineering Framework*, Bedford, MA: The MITRE Corporation, 2011.

[8] Computer Network Defense Architecture (April 2011), K. Bingham, [Online]. Available: http://www.dodenterprisearchitecture.org/pastmeetings/Documents/2011_DoD_EA_CND%20Architecture_Bingham.pdf. [Accessed 18 November 2015].

[9] G. Jakobson, "Mission resilience," in Cyber Defense and Situational Awareness, Fairfax, VA, Springer, 2014, pp. 297–322.

[10] A. Madni and S. Jackson, "Toward a conceptual framework for resilience engineering," *IEEE Systems Journal*, vol. 3, no. 2, pp. 181–191, 2009.

[11] E. Hollnagel, C. Nemeth, and S. Dekker, *The Four Cornerstones of Resilience Engineering*, Ashgate, 2009.

[12] D. Shackleford, *Virtualization Security: Protecting Virtualized Environments*, Indianapolis, IN: John Wiley & Sons, 2013.

[13] *4 Critical trends in IT business continuity*, (April 2012) CSO, 2 B. Violino [Online]. Available: http://www.csoonline.com/article/2131372/emergency-preparedness/4-critical-trends-in-it-business-continuity.html?page=2

[14] *What are the different types of virtualization?* (2 June 2008), VirtualizationAdmnin.com VirtualizationAdmnin.com, [Online]. Available: http://m.virtualizationadmin.com/faq/different-types-virtualization.html

[15] *How server virtualization works* (17 October 2015), How Stuff Works, J. Strickland, [Online]. Available: http://computer.howstuffworks.com/server-virtualization.htm

[16] *f5 White Papers* (5 December 2007), f5, A. Murphy, [Online]. Available: https://f5.com/resources/white-papers/virtualization-defined-eight-different-ways

[17] *What is the difference between presentation virtualization and remote desktop services?* (2 June 2011), WindowsITPro, [Online]. Available: http://windowsitpro.com/virtualization/q-whats-difference-between-presentation-virtualization-and-remote-desktop-services

[18] *The software designed data center* (17 October 2015), VMWare, [Online]. Available: http://www.vmware.com/software-defined-datacenter/networking-security

[19] *Virtualization security* (17 December 2012) INFOSEC Institute,. T. Komperda, [Online]. Available: http://resources.infosecinstitute.com/virtualization-security-2/

[20] *Server virtualization: Top five security concerns* (13 May 2009). K. Fogarty [Online]. Available: http://www.cio.com/article/2428191/virtualization/server-virtualization--top-five-security-concerns.html

[21] *The basics of virtualization security* (2011). C. Brenton, [Online]. Available: https://cloudsecurityalliance.org/wp-content/uploads/2011/11/virtualization-security.pdf

[22] *U.S. says Iran hacked Navy computers* (27 September 2013) Wall Street Journal J. Barnes and G. Siobhan, [Online]. Available: http://www.wsj.com/articles/SB10001424052702304526204579101602356751772

[23] *Revisiting the Navy's blueprint for cyber operations* (18 March 2015) FCW, S. Lyngaas [Online]. Available: https://fcw.com/articles/2015/03/18/navy-cyber-operations.aspx

[24] DONCIO, *Next Generation Enterprise Network: Network Operations Concept of Operations*, Washington, DC: U.S. Navy, 2008.

[25] *Cyber Attacks Top List of Business Continuity Threats for* 2015 (20 February 2015) KETCH Consulting, [Online]. Available: http://ketchconsulting.com/2015/02/20/cyber-attacks-top-list-of-business-continuity-threats-for-2015/.

[26] *CNO's navigation plan 2016-2020* (20 July 2015). A. J. Greenert, [Online]. Available: http://www.navy.mil/cno/docs/150528_cno_navigation_plan.pdf

[27] M. Nissen, *Harnessing Dynamic Knowledge Principles in the Technology-Driven World*, Hershey, PA: IGI Global, 2013.

[28] *Business Impact Analysis* (23 January 2016) Department of Homeland Security, [Online]. Available: http://www.ready.gov/business-impact-analysis

[29] B. Goldwater and W. Nichols, *Goldwater-Nichols Department of Defense Act of 1986*, Washington, DC: U.S. Congress, 1986.

[30] United States Strategic Command, *Department of Defense Information Operations Condition (INFOCON) System Procedures*, Omaha, NE, 2006.

[31] *Providing Direct Access to the NMCI Network* (2014). Hewlett Packard, [Online]. Available: http://www8.hp.com/h20195/v2/getpdf.aspx/4AA3-6482ENW.pdf?ver=1.0.

[32] A. Barreto, "Integration of virtual machine technologies into hastily formed networks in support of humanitarian relief and disaster recovery missions," M.S. thesis, Dept. of Information Sciences, Naval Postgraduate School, Monterey, CA, 2011.

[33] M. Batolacci, C. Aubrecht and D. Aubrecht, "A portable base station optimization model for wireless infrastructure deployment in disaster planning and management," Information Systems for Crisis Response and Management, 2014.

[34] RAND National Defense Research Institute, *CANES Contracting Strategies for Full Deployment*, Arlington, VA: The RAND Corporation, 2012.

[35] SPAWAR, *Consolidated Afloat Networks and Enterprise Services (CANES) Fact Sheet*, San Diego, CA: United States Navy, 2011.

[36] *Data center consolidation and optimization* (12 February 2016) CIO.gov, [Online]. Available: https://cio.gov/drivingvalue/data-center-consolidation/

[37] S. Anankar, A. Mohta, and S. Sane, "Optimization in virtualization," ThinkQuest 2010, Springer, 2010, pp. 92–97.

[38] *Virtualization* (25 January 2016) VMWare, [Online]. Available: https://www.vmware.com/virtualization/how-it-works

[39] P. Denning, "Hastily formed networks," *Communications of the ACM*, vol. 49, no. 4, pp. 15–20, 2006.

[40] *2014 Threat report* (2014), Mandiant, [Online]. Available: https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

[41] *The virtualization security landscape: What's changed?* (25 March 2012) RSA 2012, D. Shackleford, [Online]. Available: https://www.youtube.com/watch?v=WIBnLLweuFg

[42] Executive Office of the President National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, Washington, DC: United States Government, 2011.

[43] N. Provos and T. Holtz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*, Boston, MA: Addison Wesley, 2008.

[44] E. Hutchins, M. Cloppert, and R. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*" Academic Conferences Ltd, pp. 113–125, 2010.

[45] *Intrusion detection FAQ: What is a honeypot?* (12 July 2000), SANS, L. Even, [Online]. Available: https://www.sans.org/security-resources/idfaq/honeypot3.php

[46] *Security through obfuscation; A quirky case study* (19 October 2014), LinkedIn, D. L. Crites, [Online]. Available: https://www.linkedin.com/pulse/20141019034420-86405213-security-through-obfuscation-a-quirky-case-study.

[47] *Smart IDS - Hybrid La Brea tarpit* (2009) SANS, C. Ruvalcaba, 2009 [Online]. Available: https://www.sans.org/reading-room/whitepapers/detection/smart-ids-hybrid-labrea-tarpit-33254

[48] *Computer forensics: Bringing the evidence to court* (2006), INFOSEC Writers, C. Walker, [Online]. Available: http://www.infosecwriters.com/Papers/CWalker_Computer_Forensics_to_Court.pdf

[49] *Attribution is hard to do - but necessary to evaluate risk* (17 March 2015), Palo Alto Networks, R. Howard. [Online]. Available: http://researchcenter.paloaltonetworks.com/2015/03/attribution-is-hard-to-do-but-necessary-to-evaluate-risk/

[50] *Virtual DMZs in the cloud* (18 June 2014), INFOSEC Institute. [Online], Available: http://resources.infosecinstitute.com/virtual-dmzs-cloud/

[51] J. Paulenich, C. Agbedo, and K. Rea, "Identification and triage of compromised virtual machines," M. S. capstone, Cyber Academic Group, Naval Postgraduate School, Monterey, CA, 2014.

[52] C. Greer, *Government-University-Industry Research Roundtable*, Washington D.C.: White House Office of Science and Technology, 2011.

[53] Y. Huang and A. Ghosh, "Introducing diversity and uncertainty to create moving attack surfaces for web services," *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats* , vol. 54, Ney York, NY, Springer, 2011, pp. 140–151.

[54] VMWare, *VMWare vSphere vMotion Architecture, Performance and Best Practices in VMWare vSphere5*, VMWare, Palo Alto, CA, 2011.

[55] M. Lam, "Lower total cost of ownership of ONE-NET by using thin-client desktop deployment and virtualization-based server technology," M.S. thesis, Dept. Sys. Eng., Naval Postgraduate School, Monterey, CA, 2010.

[56] VMWare TCO Comparison Calculator (28 February 2016), VMWare, [Online]. Available: http://www.vmware.com/go/tcocalculator/newIndex.html?numvirtualMacin=1000&productEdition=vSphere+with+Operations+Management+Enterprise+Plus&nummacinDeploy=1000&virtualizationHost=Server+B+%28HP+DL380e+Gen8%2C+2+CPU%2C+128GB+RAM%29&networkedStorage=NAS&net

[57] *Server virtualization* (1 February 2016), Department of Energy, [Online]. Available: https://www.energystar.gov/products/low_carbon_it_campaign/12_ways_save_energy_data_center/server_virtualization

[58] M. Kuhl, J. Kistner, K. Costantini, and M. Sudit, "Cyber attack modeling and simulation for network security analysis," Proceedings of the 2007 Winter Simulation Conference, Washington, DC, 2007, pp. 1180–1188.

[59] Unified Communications in a Virtualized Environment (29 January 2016), Cisco,. [Online]. Available: http://docwiki.cisco.com/wiki/Unified_Communications_in_a_Virtualized_Environment#How_to_Buy

[60] Cicso Business Edition 6000 (28 February 2016), IPPhone, [Online]. Available: http://www.ipphone-warehouse.com/Cisco-BE6K-ST-BDL-K9-p/be6k-st-bdl-k9.htm

[61] *Riverbed modeler* (28 February 2016), Riverbed, [Online]. Available: http://www.riverbed.com/products/steelcentral/steelcentral-riverbed-modeler.html

[62] *Riverbed modeler* (28 February 2016) WANSolutionWorks,. [Online]. Available: http://www.wansolutionworks.com/Modeler.asp

[63] *Standards for computer server rooms* (24 March 2014), University of California San Diego, [Online]. Available: http://blink.ucsd.edu/technology/computers/basics/resources/servers.html#General-space-characteristics

[64] *Server room renovations and expansions* (3 June 2008), InfoTech Research Group, [Online]. Available: https://www.infotech.com/research/server-room-renovations-and-expansions-not-a-diy-project

[65] T. Housel and A. Bell, *Measuring and Managing Knowledge*, New York, NY: McGraw-Hill/Irwin, 2001.

[66] Catalog of Navy Training Courses (CANTRAC) (28 February 2016), U.S. Navy, Commander of Naval Education and Training [Online]. Available: https://app.prod.cetars.training.navy.mil/cantrac/vol2.html

[67] Chief of Naval Operations, *NAVADMIN 361/12 Sea Shore Flow Enlisted Career Paths Updates (Corrected Copy)*, Washington, DC: U.S. Navy, 2012.

[68] Navy announces award of Next Generation Enterprise Network contract (27 June 2013), Defense Media Activity-Navy, [Online]. Available: http://www.navy.mil/submit/display.asp?story_id=75100

[69] *Guidance and directives* (4 May 2007), Department of Homeland Security, [Online]. Available: http://www.fema.gov/guidance-directives. [Accessed 1 February 2016].

[70] *Navy Unit Commendation citation* (2014), Navy.mil, [Online]. Available: http://www.public.navy.mil/fcc-c10f/Fact%20Sheets/Navy%20Unit%20Commendation.2014.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California