HSSEDI
Homeland Security Systems Engineering & Development Institute

Prepared for:
Department of Homeland Security

Cyber Wargaming:
Framework for Enhancing Cyber Wargaming with Realistic Business Context

August 29, 2018

Authors:

David B. Fox
Catherine D. McCollum
Eric I. Arnoth
Darrell J. Mak

The Homeland Security Systems Engineering and Development Institute (HSSEDI)™
Operated by The MITRE Corporation

Approved for Public Release; Distribution Unlimited.
Case Number 18-1636 / DHS reference number 16-J-00184-04

Homeland Security Systems Engineering & Development Institute

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract HSHQDC-14-D-00006.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

HSHQDC-16-J-00184
Next Generation Cyber Infrastructure (NGCI) Apex Cyber Risk Metrics and Threat Model Assessment

This HSSEDI task order is to enable the DHS Science and Technology Directorate (S&T) to facilitate improvement of cybersecurity within the Financial Services Sector (FSS). To support NGCI Apex use cases and provide a common frame of reference for community interaction to supplement institution-specific threat models, HSSEDI developed an integrated suite of threat models identifying attacker methods from the level of a single FSS institution up to FSS systems-of-systems, and a corresponding cyber wargaming framework linking technical and business views. HSSEDI assessed risk metrics and risk assessment frameworks, provided recommendations toward development of scalable cybersecurity risk metrics to meet the needs of the NGCI Apex program, and developed representations depicting the interdependencies and data flows within the FSS.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information about this publication contact:

Homeland Security Systems Engineering & Development Institute

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Email: HSSEDI_info@mitre.org

http://www.mitre.org/HSSEDI

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Abstract

This report describes a framework for cyber wargaming that balances the strong cyber defense technology focus of detailed hands-on cyber red-teaming exercises with the strong business and operational impact focus typical of high-level tabletop exercises focused on cyber. While the framework was developed with a focus on securing systems in the financial services sector (FSS) and is described in terms of that domain, it is expected to be applicable more broadly, to other critical infrastructure protection sectors, as well as other types of enterprises entirely.

The report begins by providing a summary of existing cyber wargaming practices and applicable technologies before describing an alternative composite framework to serve as a basis for enhanced wargaming applicable to individual institutions or multi-institution sector operations. A key finding is that existing frameworks are sufficient to leverage in a composite cyber wargaming scenario model to produce improved realism. Consideration is given to how technologies can be used to enhance simulation and orchestration within cyber wargaming exercises, as well as measuring outcomes of such events. The report also discusses approaches for planning, preparing, and conducting cyber wargames using the integrated scenario framework. These approaches could be used to extend and enhance existing wargaming practices an organization may already have implemented. The initial framework presented in the report is general and intended to be tailored to ensure that wargaming exercises accurately reflect the effectiveness of an institution's risk management and technology environment in reducing the impact and risk from cyber adversaries.

Key Words

1. Cyber Wargaming Scenarios
2. Cyber Wargaming Framework
3. Cyber Wargaming Methodology
4. Threat Vector Models
5. Cybersecurity

Executive Summary

Cyber wargaming, based on business process models and technology-aligned penetration testing or red teaming of technology platforms, has been used for some time both to provide an assessment of deployed technology and as a learning activity. Findings from cyber wargaming can be used to improve event response, platform and application development, selection and integration of defensive technologies, and deployment compliance to reduce risk. Metrics from these events are typically relative measures of the results within the testing scope, often limited to a single organization or small group engaged in coordinated exercises.

This report considers opportunities for improving this activity through scenarios that more strongly integrate business activities and technology operations in relation to a realistic and repeatable simulation of sophisticated adversarial cyber events. When mapped against a framework of threats to business functions, measures of the effectiveness of the deployed risk mitigation processes and technology can be leveraged to better inform future investment choices. Scenarios can be expanded to include multiple organizations within an industry to provide insights into the effectiveness of specific products and processes for cyber defense in a broader context.

Scenarios based on actual business functions linked to organizationally deployed technologies can provide a realistic simulation of the impacts of cyber events on business operations. Scenarios that integrate elements from both current tabletop "what-if" exercises and technology-based red team exercises draw an association between the cyber defense and business process effects to examine a realistic view of an event outcome. Deriving outcomes based on the realistic variability of actual controls, management decision-making, deployed infrastructure, third-party dependencies, and multi-party disruptions across a business sector can identify a broader range of gaps in operational resiliency. Establishing a systematic, repeatable, and measurable model for cyber wargaming integrating business and technology views can provide better insights on potential benefits of acquisition of new technologies and their lifecycle management.

Table of Contents

1 Introduction 1
1.1 Objectives 1
1.2 Uses of Cyber Wargaming 2
1.2.1 Assessing Capabilities 2
1.2.2 Planning 2
1.2.3 Training 2
1.2.4 Systemic Risk Identification 3
1.3 Outline of Report 3
2 Background 5
2.1 Levels of Cyber Wargaming 5
2.2 Key Elements of Cyber Wargaming 6
2.3 Player Organization within Cyber Wargaming 7
2.4 Cyber Wargaming at a Composite Level 9
2.5 Cyber Wargaming Success Factors 10
2.6 Cyber Wargaming Reference / Abstract Model 12
2.7 Wargaming Limitations 13
3 Cyber Wargaming Technologies and Components 15
3.1 Frameworks and Models 15
3.1.1 Wargame Construction Kit 15
3.1.2 Business War Games 15
3.1.3 Commercial Offerings with Proprietary Toolkits 16
3.2 Platforms 16
3.2.1 Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE) 16
3.2.2 Maelstrom 16
3.2.3 Cyber Gym 17
3.2.4 SimSpace 17
3.2.5 Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA) 17
3.3 Exercise Environments and Tools 17
3.3.1 Fort Meade Experiment (FMX) 18
3.3.2 National Cyber Range 18

3.3.3 Lincoln Adaptable Real-Time Information Assurance Testbed (LARIAT) 18
3.3.4 SimSpace 18
3.4 Simulations 18
3.4.1 Analyzing Mission Impacts of Cyber Actions (AMICA) 19
3.4.2 Hacknet Labyrinths 19
3.5 Adversary Emulation 19
3.6 Exercises and Scenarios 20
3.6.1 Hamilton Series 20
3.6.2 Quantum Dawn Series 20
3.6.3 RSA 2016 20
3.6.4 RSA Singapore 2016 20
3.6.5 DHS Cyber Storm Series 21
3.6.6 BSides Las Vegas 21
3.6.7 Bank of England Series 21
3.6.8 Capture-the-Flag Events 22
3.7 Portraying Defensive Capabilities 23
3.7.1 Cyber Analytic Repository (CAR) 23
4 Applying Composite Cyber Wargaming to Financial Services and Other Sectors 24
4.1 Cyber Wargaming Objectives 24
4.1.1 National Level Objectives 24
4.1.2 Sector-Level Objectives 25
4.1.3 Individual Institution Objectives 26
4.1.4 Public 26
4.1.5 Technology 27
4.2 Composite Model Rationale and Measures of Success 27
4.2.1 Spectrum of Wargame Levels 29
4.2.2 Scenario Development 32
4.2.3 Existing Capabilities and Gaps 33
4.3 Technology Mapping to Composite Cyber Wargaming Elements 34
5 Enabling Capabilities for Testing and Wargaming 36
5.1 Game Structure 36
5.1.1 Process Overview 36
5.1.2 Adversary Attack Options 37

5.1.3 Business Functions 39
5.1.4 System and Application Mapping 41
5.1.5 Product Threat Mitigation Evaluation 42
5.1.6 Defensive Capabilities 43
5.1.7 Resiliency Response Actions Playbook 45
5.2 Wargaming Platform Requirements 45
5.2.1 Orchestration 45
5.2.2 Measures and Metrics 45
6 Composite Cyber Wargaming Scenarios 47
6.1 Developing Wargaming Scenarios and Gaming Strategy 47
6.2 Example High-Level Composite Scenario 49
6.2.1 Scenario 50
6.2.2 Scenario Elements 51
6.2.3 Metrics 52
6.2.4 Exercise Objectives 52
6.2.5 Wargaming Actions 52
6.2.6 Exercise Participants 56
7 Summary and Conclusions 58
7.1 Composite Cyber Wargaming Strengths 58
7.2 Composite Cyber Wargaming Limitations 59
7.3 Changing Threats and Emerging Technologies 59
Appendix A Planning, Conducting, and Assessing a Composite Cyber Wargame 61
Appendix B Example Events and Actions 65
List of Acronyms 67
List of References 72

List of Figures

Figure 1. Cyber Wargaming Reference Model 12
Figure 2. ATT&CK Framework Post-Compromise Adversary Tactics 44

List of Tables

Table 1. Contrasting the Three Classes of Cyber Wargames 9
Table 2. Defender Effectiveness Measures 28
Table 3. Attacker Effectiveness Measures 29
Table 4. Integration Levels 30
Table 5. Alternatives for Implementing Wargame Elements 35
Table 6. Product Survey Example 42
Table 7. Use of Effectiveness Values 43
Table 8. Defensive Technology Platforms Mapped to Carbanak TTPs 51
Table 9. Wargaming Actions for Sample Scenario 53
Table 10. Exercise Participants 56
Table 11. Example Events and Actions 65

1 Introduction

Cyber wargaming is a technique for examining what would happen in a particular organizational and systems context if it were confronted with a variety of actual or hypothetical cyber attacks. In [Deloitte 2014], cyber wargaming is defined as "an interactive exercise that immerses participants in a simulated cyber attack scenario, such as a data breach, website defacement, denial of service attack, or the discovery of sophisticated malware on a corporate network." In this report, we take a broad view of the form such a "simulated" cyber attack scenario can take, encompassing anything from a high-level description of an event notionally taking place to hands-on execution of attack software against a system under controlled conditions by staff members emulating a real or potential cyber adversary.

Cyber wargaming is a tool that is useful to organizations for assessing current and future capabilities, planning, examining possible scenarios, and training staff. This report briefly reviews the current state of cyber wargaming, evaluates its present uses and limitations, and seeks to make the case for a new form of cyber wargaming exercise that bridges the divide between existing models. It then explores means of implementing such a composite cyber wargaming model. To illustrate how this type of cyber wargaming would be applied and implemented, it provides a number of example scenario models. By looking for potential synergistic elements that would support improvements in simulation and establish repeatable cyber attacks, it may be possible to measure the effectiveness of products and processes in withstanding or countering such attacks or minimizing the effects on ongoing business operations, across multiple entities within an organization, as well as across multiple organizations.

The report briefly reviews what kinds of cyber wargaming events are being used in the Financial Services Sector (FSS), and elsewhere. Common practice in these environments includes the use of tabletop cyber wargaming, largely with high-level scenarios focused on business process and interaction in the face of a cyber challenge, as well as detailed level hands-on testing of technical cyber defenses.

A valuable opportunity exists for combining these two approaches to gain new benefits and insights. This report explores the opportunities and challenges presented by such an endeavor and proposes means by which such a composite approach could be achieved.

1.1 Objectives

Cyber wargaming provides a method of exercising and examining, in a modeled environment, human performance and decision-making or system characteristics and outcomes, in the context of a cyber attack scenario. The cyber wargame involves interaction between adversary teams conducting cyber attacks and an enterprise seeking to defend against them while continuing to conduct its core business functions. Wargaming has a long history of use in military planning, assessment, and training but applies naturally to cyber defense as well, because of its adversarial nature. Thus, it is increasingly relevant in all sectors due to the opportunities that computer networks afford for adversaries to attack any institution.

The scope of this report is the application of wargaming specifically to cyber defense to maintain successful business operations, rather than more broadly to other organizational objectives and challenges as in military wargaming.

1.2 Uses of Cyber Wargaming

As noted, cyber wargaming can be put to a number of uses, including assessing the effectiveness of current capabilities against cyber attack, examining potential additions or changes for planning purposes, providing key staff members with the experience of being confronted by a cyber attack, and, when applied to multiple organizations with identified interdependencies, helping to identify systemic risks due to cyber attacks.

1.2.1 Assessing Capabilities

One of the key organizational objectives for cyber wargaming is to support assessment of current capabilities. Planned and controlled wargames present a unique opportunity to identify the strengths and weaknesses of an organization's network and systems architecture, its defensive technologies, and its processes and procedures. By subjecting the current defensive regime to cyber attacks in a simulated environment, valuable lessons can be learned with minimal risk. After the exercise, review with the team playing the part of the adversary of what happened and what could be done better to defend the system more effectively is a valuable opportunity that has few parallels in other venues. Without this evaluation forum, few opportunities exist for an organization to objectively and holistically determine the strengths and weaknesses of their current capabilities, other than by experiencing an actual breach.

1.2.2 Planning

As a natural outgrowth of assessing current capabilities, organizations also tend to utilize cyber wargaming to plan for the future. This can constitute looking ahead towards future technical capabilities, changes in technical practices and procedures, or evaluating strategy and architectural changes. To assess future technical capabilities, new or even envisioned technologies can be fielded in the wargaming environment (or modeled) and put under the duress of realistic cyber attack scenarios. Similarly, by emulating planned changes in practices, procedures, strategy, and architecture and subjecting them to cyber attack in the wargaming environment, an organization can simulate the effects and impacts of changes under consideration before actually spending the time, effort, and capital to implement them in the field. This also presents the opportunity to identify new risks incurred with new approaches and capabilities, rather than learning of them after deployment in live business function environments.

1.2.3 Training

While other training venues exist, such as computer-based training (CBT), instructor-led seminars such as those offered by the System and Network Security (SANS) Institute, or cybersecurity certifications, none of these options offer the same sort of simulations of real-world experiences that happen with a cyber wargaming event. In an actual major cyber attack on

an organization, considerable stress is placed upon the employees and managers who are faced with a live adversary operating in real-time. In a cyber wargaming scenario, this exact formula is reproduced, with many of the same pressures and rapidly occurring events that compete for people's attention and focus. In a well-orchestrated event, participants will feel like they are in a real-world situation. This presents the opportunity for learning how well staff and management will perform under fire, while simultaneously assessing the strengths and weaknesses of their skills and helping them improve their skills or self-identify areas of needed improvement.

1.2.4 Systemic Risk Identification

An important aspect of cyber wargaming is to identify risks that cross organizational boundaries and may undermine resiliency in business functions. Threats that are applicable across multiple organizations within a Critical Infrastructure[1] (CI) sector result in systemic risk. Areas for consideration in cyber wargaming exercises that may contribute to systemic risk are:

- Lack of diversity in technology, and common vendor and technology product performance failures, such as those seen through open source software and Windows vulnerabilities
- Reliance on third parties to support organizational business functions
- Failure to leverage other sector members to provide temporary backup and business diversity for business functions to counter cross-sector events
- Delayed response and decision-making due to lack of effective communication or clear definition of responsibilities
- Misinformation or lack of data to support development of courses of action to mitigate malicious activity.

1.3 Outline of Report

The remainder of this report explains and illustrates a framework for enhanced composite cyber wargaming in support of these uses, as follows:

- Section 2 provides background on cyber wargaming and introduces the notion of a composite cyber wargaming framework using scenarios that integrate business and technical perspectives.
- Section 3 briefly reviews existing cyber wargaming frameworks, applicable technologies, and cyber wargaming exercises.
- Section 4 examines the application of composite cyber wargaming to the FSS, and ultimately other environments.

[1] Department of Homeland Security Critical Infrastructure Sectors, https://www.dhs.gov/topic/critical-infrastructure-security, National Infrastructure Protection Plan, https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

- Section 5 discusses enabling capabilities for testing and composite cyber wargaming.
- Section 6 defines the components of integrated scenarios for composite cyber wargaming and provides examples.
- Section 7 concludes the report.
- Supporting information is provided in the Appendices.

2 Background

Before examining relevant technologies and models, it is useful to summarize some characteristics of cyber wargaming exercises, including level of detail, objectives, types of participants, and scope. Additionally, capability gaps of the wargaming scenarios are discussed.

2.1 Levels of Cyber Wargaming

Definitions of the term cyber wargaming vary, but the concept is readily applied to both tabletop exercises and red-team exercises.

- In tabletop exercises, the gameplay is highly abstracted and participants are presented with predetermined scenario events (in paper or automated form) to react to. These exercises are often single-sided, meaning that the exercise includes only the defending team. The adversary is then represented through the scripted scenario events, rather than via an opposing team participating in the game.
- Red-team exercises are two-sided and take place in a much more concrete, real world environment. In a red-team exercise, a human team playing the part of a cyber adversary performs live attacks on an actual information technology system, in a laboratory, testbed, or real operational environment, while human defenders seek to discover their activities and prevent them from achieving their goals.[2]

Some degree of simulation can also be incorporated in either type of exercise.

Often, tabletop-style exercises focus on high-level incident coordination, decision-making, planning, and management of impacts on business functions, while red-team exercises focus on the technical details of the attack exploits, the usefulness of cyber defense technologies, and the effect of defenders' actions in preventing, detecting, and reacting to attacks and breaches. A third type of exercise appears potentially valuable, conducted at an intermediate level of detail and focused on bridging between the specifics of cyber technologies and the business function implications.

As a means to bridge the gap between high-level tabletop-style exercises and hands-on technical red-team exercises, a composite middle tier that borrows from both ends of the spectrum may be possible. This middle tier would combine business processes with simulated technologies and technical events. By creating a simulation, the middle-tier exercise would allow for some level of spontaneity in how adversaries and defenders respond to each other, while also allowing for the incorporation of higher-level impacts such as business outages or customer impact. This new type of wargaming would provide greater technical realism than is typically available in table-tops, without incurring the cost and effort required for a full-spectrum red-team exercise.

[2] Terms other than red teaming are sometimes used, such as live exercises, hands-on cyber exercises, capture the flag, or ethical hacking.

2.2 Key Elements of Cyber Wargaming

Cyber wargaming exercises include the following key elements. The prevalence and depth of particular elements can vary from one type of exercise to another, but they are all addressed in some form. Both tabletop and red-team exercises likely will make assumptions about the mapping of technology support to business function as part of a cyber impact scenario.

- **Scope**. The scope of an exercise is shaped by its objective. The defined scope includes the organizational and networked information technology (IT) system contexts. For instance, the organizational scope of FSS institutions might be a sub-organization or line of business within the institution, the entire institution, a FSS subsector function that spans multiple institutions, the entire FSS, or the FSS in relation to other critical infrastructure sectors. The scope of the networked IT systems to be included in the exercise is dictated by the organizational scope.
- **Business Functions**. Most cyber wargaming goes beyond simply whether a vulnerability exists or a particular exploit can be run and examines how some level of business functions can be affected. These could be anything from quite low-level functions, such as performing an on-line banking transaction, to strategic operations within an institution such as conducting mergers and acquisitions support, to multi-institution functions such as payments processing. Whatever the level, the business functions are defined and represented in the cyber wargame in some way. Business functions include users, procedures, automated business applications, and information assets.
- **System environment**. The IT system environment, although it may be very abstracted in the case of a tabletop exercise or an actual testbed emulation in the case of a red-teaming exercise, is a critical element in cyber wargaming. The system environment in large part determines what portfolio of attack strategies and mechanisms are relevant, and what interconnections are available to allow attackers to move from an initial entry point towards targeted assets. The system environment includes the networking components, user endpoints, application and data servers, topology, and external connections.
- **Defensive cyber technologies and posture**. Organizations need to continuously learn what an adversary could do despite the security measures in place. In order for the cyber wargame to be relevant to a realistic situation, the cybersecurity protections built into the IT environment, such as segmentation, firewalls and filters, endpoint security configurations, authentication, and access control must be captured in the system model used in the wargame. In addition, the organization's cyber defense toolset, such as detection sensors and cybersecurity monitoring and management tools must be represented. These must include cyber defensive capabilities within the defended network and systems, not just at perimeters. Part of the wargame involves dealing with adversaries that have already penetrated the perimeter, through various means, and are operating within defended assets.
- **Threat**. A specific threat model is a necessity for cyber wargaming. To be most effective, the type of adversaries targeting the organizations' IT environments in the wargame should be defined, along with their specific goals and capabilities. (Threats can also

include non-human generated threats, such as a natural disaster, either as a standalone threat or in conjunction with other threats.) The threat need not be restricted to what the organization has actually experienced in the real world. A cyber wargame can posit a level of adversary capability that the organization has not yet seen in practice, and in fact it can be important to explore how well the organization's cyber defenses and staff would react to such a challenge. However, little can be learned from a cyber wargame in which the threat is either underestimated and limited to trivial opportunistic attacks, or exaggerated and able to perform unrealistic and infeasible attacks.

- **Scenarios**. A scenario provides the story that participants experience and react to during the cyber wargame. The scenario identifies what the specific situation is: what is going on in the business context, who the adversary is, what assets are targeted, and to what purpose. The scenario may also specify how the adversary harms the organization using the access gained, results of cyber attacks mounted against other organizations, real-world actions taken in connection with the cyber attack, information being reported in the press or through threat intelligence sources, and how the adversary either escalates the intensity of their efforts or pursues alternate attacks if the attack is frustrated.

2.3 Player Organization within Cyber Wargaming

Multiple human teams take part in a cyber wargame with different roles. As an artifact of their origin in the military, they follow a color-based naming convention. The blue team represents the organization's own staff, while the red team represents the cyber adversary. The white team is associated with neither side but provides necessary support to the wargame. The size and exact skillset of the teams will vary depending on whether the wargame is a scripted tabletop interaction or an actual exercise with live attacks in a testbed, but each of the following roles is needed in some form.

- **Blue team: Cyber defense**. The cyber defense team includes participants in the wargame who staff the IT environment's cyber defenses. They perform the processes of the organization's cyber defense operations. They receive inputs from detection systems and threat intelligence, try to diagnose and interpret the associated attack activities, investigate incidents, and respond when needed by initiating cyber defense actions against the attack (such as blocking, or collecting further information) or by reconfiguring the security posture.
- **Blue team: Business operators**. Other important members of the blue team are participants who are knowledgeable of the business functions and applications of the organization's IT environment, rather than being specialists in details of cybersecurity. Depending on the nature of the cyber wargame, these participants may represent different levels of the organization. For detailed red-team exercises, participants represent the staff who have a job to get done using the IT system. The system capabilities they operate provide the context within which attacks take place. They are particularly important for two reasons. First, if the game lacks realistic business function activities and workloads taking place in the systems and network, cyber defenders have a quiet environment that may render attacker activities easier to discover. Second, if attacks slip through the cyber

defenses undetected, the only evidence is likely to be in the effects they have on business data and functions, which only participants versed in the business operations may notice. For tabletop exercises focusing on higher level coordination and incident response, participants representing senior management IT and business executives are likely to be needed. When cyber defense actions are considered, the decision-making process needs to consider effects on the broader goal of keeping the organization's business functions operating successfully. In addition, these participants are the decision-makers for coordination and information dissemination, including cooperation with regulatory authorities, law enforcement, and affected peer companies, as well as the public, if needed.

- **Red team**. The red team is responsible for emulating the behavior and capabilities of the adversary specified in the threat model. Depending on the threat model and scenario, the adversary's behavior may be aggressive or risk-averse or somewhere in between. They may seek to attack while evading detection or to attract attention and intimidate. They may use cyber access gained to damage the system, and thereby the organization's business functions in obvious or subtle ways, or simply to spy and extract information. A cyber wargame might include a single adversary (of one or more people working together), two or more colluding adversary teams with distinct identities and practices, or multiple unrelated adversary teams targeting the organization for their own separate goals. It is important to view the red team as an integral part of the game support staff that actively collaborates, throughout the exercise, to help the white team meet the game's objectives.
- **White team**. The white team provides support functions needed in the operation of a cyber wargame. They serve essentially as the referees and support staff of the technical aspects of the game. No cyber wargame can fully specify and anticipate all possible circumstances and questions that arise when the participants become engaged in a scenario. Before the cyber wargame, the white team defines the rules and sets bounds on what is allowed and not allowed. (In the case of red-teaming, they determine what red team tactics and methods are allowable and set literal bounds on the network address ranges within which the red teams are permitted to manipulate systems and mount attacks.) As the cyber wargame is conducted, the white team interprets unclear or ambiguous events, responds to questions for which data has not been prepared, and monitors the activities of participants to ensure they are acting within the rules.
- **Test Director**. The test director controls the progress of the cyber wargame. The test director monitors and may intervene to influence the pace of play to ensure that the cyber wargame objectives are met within the time allotted. Depending on how the game is progressing, and whether particular issues are being explored to the extent desired, the test director may have the option to inject additional events into the situation or subtract others that had been planned. The test director is also responsible for data collection about the cyber wargame, possibly in conjunction with a team of observers, as well as post-analysis and reporting out.

In addition, the following optional roles may be appropriate. Not all of these roles will be appropriate for all games, whether tabletop or red team exercises. The groups conducting the exercise in question should use their discretion to involve the roles appropriate for the goals and objectives of the event.

- **Threat Intelligence**: Many organizations subscribe to commercial threat intelligence feeds to help them identify malicious activity within their networks. Players within the game could serve in the capacity of intelligence brokers, disseminating tips and Indicators of Compromise (IOCs) about the Red Team.
- **Law Enforcement Officers (LEOs)**: Often in the real world during a cybersecurity breach, interaction with law enforcement is either unavoidable or even desirable. Having a player group to play the part of law enforcement can help to better facilitate simulations of these interactions, identifying the challenges and benefits of such options during an event.
- **The Media**: In some cases, a cybersecurity incident will lead to public disclosure. Such disclosures will inevitably involve public awareness being disseminated through news outlets. A player group to play this role will enable the Blue Teams to experience the interaction of being contacted for comment and will force those in a management role to decide how to respond and perhaps even try to shape the story.

2.4 Cyber Wargaming at a Composite Level

As noted in Section 2.1, it appears there is value in cyber wargaming at a third level that bridges between the business-impact focus typical of tabletop exercises and the concrete technical focus of red-teaming events. We refer to this third level as composite cyber wargaming. Table 1 provides a summary of how composite cyber wargaming fits between the more common models of tabletop and red-team exercises, fusing some of their aspects.

Table 1. Contrasting the Three Classes of Cyber Wargames

Game Aspect	Tabletop	Composite	Red-Team Exercise
Typical primary participant level	Executives	Executives and mid-level cyber and business staff	Working level cyber staff
Purpose	Test organizational incident response and reaction to protect business in a cyber-caused crisis	Test ability to withstand and counter goal-oriented scenarios and business-targeted effects; Identify gaps in capability, technology, training, and experience of cyber staff.	Test ability to recognize and counter exploits and expunge attacker footholds; Identify capability and technology gaps
Focus	Communication, coordination, macro-level business decisions and actions (the war)	Escalation; mapping to business impacts; technologies, processes, and tradecraft to recognize attacks or carry out courses of action (the battle)	"Point" cyber technologies and correlation (the hand-to-hand skirmish)

Game Aspect	Tabletop	Composite	Red-Team Exercise
Results	Identify effectiveness of reporting practices and policies in supporting business decision-making in cyber context	Identify effectiveness of cyber tools in supporting cyber analysis and decision-making about cybersecurity issues in the business context	Identify effectiveness of cyber tools and technical vulnerabilities of system
Activities	Understand source (attack agent) and motivation; Decide what to do or choose not to do; decide when to escalate (i.e., if nation-state); Coordinate response, share intelligence, and communicate with internal and external stakeholders	Understand attack vector; Assess, decide and direct further defense or information gathering, decide when to escalate; Coordinate response, share intelligence, and communicate with internal and external stakeholders	Understand attack vector; Take technical actions to detect, hunt, protect, gather info; decide when to escalate; Coordinate response, share intelligence, and communicate with internal and external stakeholders
Challenges (for players)	Changing or even false information Changing/progressing situation	Changing or even false information Changing/progressing situation	Changing or even false information Changing/progressing situation
Adversary representation	(Often) Planned scenario	Participants emulating adversary, business-oriented goal and attack vocabulary	Red team, live fire

2.5 Cyber Wargaming Success Factors

A cyber wargame, of whatever level, is a significant investment of time and effort. (An overview of the tasks required to plan, conduct, and assess a composite level wargame is provided in Appendix A). Success can be assessed against measures such as the mitigation of a technical compromise, the reduction of a business impact, or some derivative of an adversarial event. The following are factors that have a significant bearing on the success of a cyber wargame.

- **Cost**. Cyber wargaming can be an expensive endeavor, and the organization must be prepared to accept the costs to obtain the benefits. Costs incurred are likely to include those for tools and testbed, for hiring external subject matter experts, for preparation and planning, and the opportunity cost of the time spent by participants from the organization's own staff. Costs can vary significantly, for instance, between a simple tabletop exercise involving a single organizational component and a multi-organization live event. The costs will also be influenced by the other success factors discussed below. If the anticipated costs outweigh the value of the cyber wargame objective and expected outcome, then adjustments need to be made. On the other hand, real benefits could be obtained. For instance, if the cyber wargame enables an organization to assess the value of an additional cyber technology capability or strategy before going to the expense of

acquiring, testing, deploying, and staffing it, then the event may be less costly than other methods of achieving the same goal.

- **Realism and fidelity**. The planning of the cyber wargame should take into consideration what level of realism and detail is necessary to achieve its goals. For instance, if the goal is to explore the effectiveness of different high-level cyber defense strategies, then mapping out system configurations and attack exploits in great detail may not help and may actually hinder the participants in understanding the essential aspects of the situation. A wargame focused on the specifics of a technology, by contrast, will be ineffective if it does not include enough detail to represent the relevant technical conditions and behaviors. At whatever level of detail, however, a cyber wargame is a model, and it is critical that the model be well thought out, accurate at its chosen level of precision, and that it capture the essentials that will exercise and guide the participants' options and decision criteria.
- **Scenario preparation**. The preparation of the scenario that will guide events in the cyber wargame is often a substantial part of the effort and is essential to its success. It may need to specify everything from the geopolitical backdrop to the past history of the defending institution and attacker to the specific business conditions and functions going on during the game to the attitudes and coincident behaviors of ordinary employees. It needs to define the roles being played by particular participants, the decisions they would be called upon to make, the information they would need to have, and the sources from which they could get all or part of it. Depending on the nature of the game, it may be important that it present participants with partial, conflicting, and misleading reports, as might happen in a real situation. It must do all of this to a level that is at least plausible enough to be accepted by the participants and not become a distracting factor that can, at worst, cause them to mentally reject the situation and take their minds out of the game.
- **Attacker preparation**. The role of an attacker is imperfectly represented in the short duration of a cyber wargame. Real-world attackers can spend months or years gathering information about a business and its IT environment from various sources, probing the system, and assessing how best to attack it. One way to provide a better approximation of this kind of preparation is to furnish the red team beforehand with detailed information about the IT environment, its systems, business functions, and users. In the case of a live red-teaming cyber wargame exercise, the attacker team may sometimes be given a period of time to use tools to perform reconnaissance or even penetration of the systems as configured before the actual gameplay begins.
- **Knowledgeable players**. It is imperative that participants in each of the defined roles for the cyber wargame have the appropriate skillsets and be knowledgeable in their domains of expertise. Unless the cyber wargame is being conducted specifically for the purpose of training or assessing knowledge gaps, this is a case in which it could be said that what you get out of it is what you put into it. In other words, the quality and validity of the insights gained by conducting the wargame will depend strongly on the capabilities and knowledge of the people who participate in it.

Finally, a post-game assessment session is typically held with all participants, in which the results are discussed, and their reactions and suggestions are solicited. This post-game session, or "hotwash," as it is sometimes called, is a critical part of the learning process to identify for the participants the areas in which they need to improve their skills and practices. It is also essential to the satisfaction of the participants and the ability to collect lessons learned to improve.

2.6 Cyber Wargaming Reference / Abstract Model

A conceptual reference model can help to clearly characterize the components of any cyber wargame, be it tabletop, composite, or red-team based, allowing the roles of particular technologies and processes in a potential wargaming approach to be delineated. Figure 1 offers such a reference model.

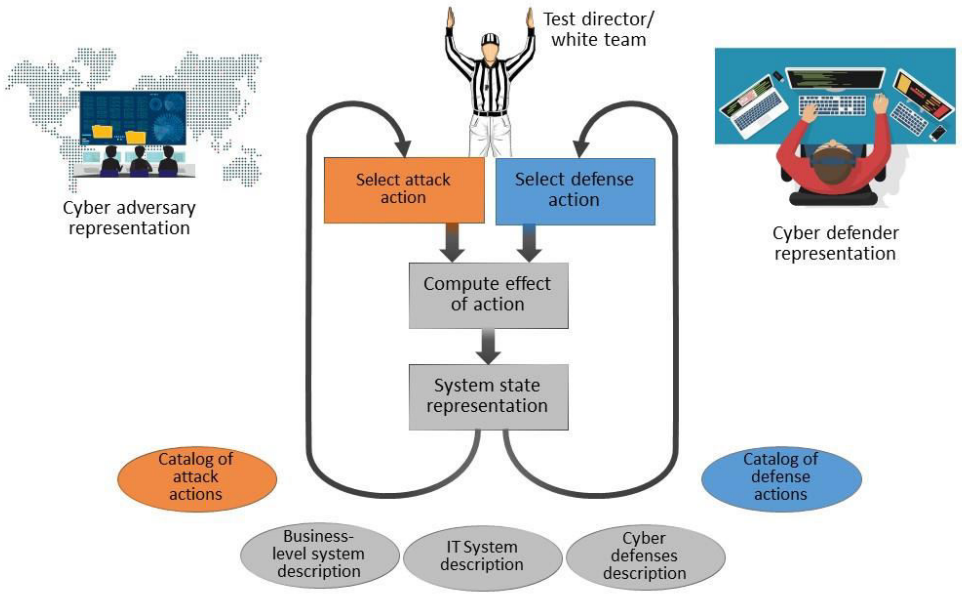

Figure 1. Cyber Wargaming Reference Model

The figure represents both the process flow of a cyber wargaming exercise and the key entities involved. The exercise platform or environment incorporates models of the business processes, the IT system that supports them, and the cyber defense systems, technologies, and processes. It uses them to maintain a representation of the current state of the system, incorporating impacts from actions taken by attackers or defenders. In the case of a red-team exercise, the actual system in the test or production environment, rather than a model, would serve as the representation of state.

The specific event would be designed and constructed by the test director and the white team. During execution of the exercise, those playing the various roles would interact with the system, whether through a dialog with the white cell or invoking predefined actions on paper in the case

of a tabletop or through interaction with the game environment or production systems in a red-team exercise. Depending on the nature and extent of the wargame, the roles of various participants could be played either by human teams or by some form of simulation that selects actions as part of the gameplay.

From the start of the activity, the cyber adversary representatives would choose actions which may or may not present the cyber defenders with evidence of hostile activity. For their part, the cyber defenders would choose to perform activities such as hardening the environment, monitoring detection systems, or responding to any evidence of a breach. Each side would have a catalog of activities to choose from, each with precomputed (or straightforwardly derivable) impacts and results that would result after selection, though these pre-ordained results would not be made known to the players in advance.

As each side performs their activities, the game would consider the effects of those actions and update the system state maintained by the wargaming platform, whether through a white team judgment, a simulation component, an actual action performed on the target system, or some combination. Impacts to the business level systems, cyber defenses, and IT systems would be considered and provided back to the players as new feedback for them to consider as they choose their next actions. Throughout the activity, the test director and white team would monitor the game's progress, adding new stimuli and tuning the system as required by the chain of events.

Not shown in the figure but also an important function of the cyber wargaming platform is recording of all activity and results, both to provide live metrics during the exercise and for reporting after the event has completed. The reporting can be used during the post-exercise hotwash session for both sides to review together. The cyber wargame organizers can use the data to better plan and prepare for future events, as well as performing fixes or improvements in the system used to operate the event.

2.7 Wargaming Limitations

Although wargaming exercises provide an excellent means to test reaction to threats and events, they have some limitations, including:

- Being played in a highly controlled environment, which inhibits the ability to perfectly mimic real-life events, where actual actions, situations, and attitudes may be quite different
- Lacking the ability to fully assess participants' spontaneity, preparedness and reaction to real-life events and surprises and thus not providing a true test of a crisis, emergency, security or system's capabilities
- Not providing a practical way to demonstrate system overload since production systems are not actually being impacted
- Not fully representing threats that are best addressed by government entities, such as nation-state-sponsored military or terrorist level capabilities not commonly available through malware marketplaces, which may be very closely held.

- Being unable to represent changing techniques and technologies. As defenders develop new methods to stop the latest attacks, adversaries are creative and are always finding new attack vectors to use. Exercises cannot reduce the risks posed by unknown, changing and evolving attack vectors (e.g., new attack vectors as a result of the explosive growth of the Internet of Things).

3 Cyber Wargaming Technologies and Components

This section describes building blocks potentially applicable to cyber wargaming related to the FSS and briefly reviews existing exercises. Each is described, and known uses are outlined, including:

- Frameworks and models for defining wargames
- Platforms for implementing and conducting wargames
- Exercise environments and tools
- Simulations applicable to wargaming
- Adversary representations
- Existing exercises and scenarios.

3.1 Frameworks and Models

The following section outlines frameworks and models that have been identified through this study. These often form the basis for adaptation of cyber specific wargaming scenarios.

3.1.1 Wargame Construction Kit

The Wargame Construction Kit is a toolset for developing tabletop military wargames [Perla 2002]. Developed as part of an instructional curriculum for wargame development, it provides rules, scenarios, terrain maps, and game pieces that can be selected and assembled to create a tailored wargame. This toolset could be examined for the extent to which it could be applied and adapted to a cyber, rather than physical military, wargame.

3.1.2 Business War Games

The book, *Business War Games*, *How Large, Small, and New Companies Can Vastly Improve Their Strategies and Outmaneuver the Competition* [Gilad 2009] outlines the use of wargaming strategies to exercise proposed business plans against competitors. It seeks to adapt military-style wargaming concepts to test an operational model against possible competitor moves. This includes identification of teams and roles, as well as identification of potential adversarial entities.

3.1.3 Commercial Offerings with Proprietary Toolkits

The construction and execution of cyber wargames is increasingly a commercial service offering. See, for example, Cisco's Cyber Range,[3] Deloitte's offering,[4] the offering by Optimal Risk,[5] Unisys's cyber resilience wargame service,[6] and PwC's Game of Threats™.[7] However, such offerings rely on proprietary frameworks and tools.

3.2 Platforms

The following section outlines the platforms designed to facilitate wargaming elements and simulation that have been identified through this study.

3.2.1 Distributed Environment for Critical Infrastructure Decision-Making Exercises (DECIDE)

Distributed Environment for Critical Infrastructure Decision-making Exercises (DECIDE) is a multi-participant cyber wargame platform developed by Norwich University Advanced Research Institute (NUARI) (http://nuari.org). Tabletop-style wargaming scenarios are added to the application and presented via a graphical user interface. Responses to white-card execution are recorded by the participants, and relayed by the application to other participants for interaction and coordination in accordance with the scenario. Participant updates and/or administrator updates drive the sequential exercise steps.

3.2.2 Maelstrom

Maelstrom [Steiger 2016] is a board game that was developed around the theme of advanced adversary activity in attacking a defended network. It was based upon the Lockheed Martin cyber kill chain lifecycle model for cyber attacks [Lockheed 2012] and MITRE's Adversarial Tactics, Techniques & Common Knowledge™ (ATT&CK™) (https://attack.mitre.org) [Strom 2017], Common Attack Pattern Enumeration and Classification™ (CAPEC™) (https://capec.mitre.org),and Cyber Resiliency Engineering Framework [Bodeau 2011]. ATT&CK is a populated threat model and framework that captures detailed tactics and techniques used by cyber adversaries operating within an enterprise network. CAPEC is a model and catalog of attack patterns.

The game has multiple levels of difficulty, allowing two or more players to assume the roles of attacker and defender. Players representing attackers attempt to move through the steps of the

[3] https://www.cisco.com/c/dam/global/en_au/solutions/security/pdfs/cyber_range_aag_v2.pdf and https://www.cisco.com/c/dam/en/us/products/collateral/security/spa-overview.pdf

[4] https://www2.deloitte.com/us/en/pages/risk/articles/cyber-risk-services-cyber-war-gaming.html and https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-cyber-war-gaming-sales-sheet-07272014.pdf

[5] http://www.optimalrisk.com/Advanced-Cyber-Defence-Services/Cyber-War-Games

[6] http://assets.unisys.com/Documents/Global/POVPapers/POV_170029_CyberResilienceServicesUnderstandingPotentialThreats.pdf

[7] https://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html

cyber kill chain to reach the "Action on Objectives" goal, while the defending players attempt to stop their progress through various response actions. Game-play takes place on a game board with cards, dice, game pieces, paper, pens, and play money. The cards present the actions that attackers and defenders can take, with a balance of the role of technology and tradecraft. The game is downloadable from https://github.com/maelstromthegame/defcon24.

3.2.3 Cyber Gym

Developed by an Israeli company, Cyber Gym (https://www.cybergym.com/) is being used to facilitate tabletop exercises in European and United Kingdom financial services organizations. Predominantly a training platform, it uses a hands-on application to simulate cyber defense and attack scenarios tailored by the company to the specific exercise. It incorporates red team, blue team, and management/white team roles.

3.2.4 SimSpace

SimSpace (https://www.simspace.com) was formed to commercialize and extend government-funded technologies for cybersecurity testing, including benign and attack traffic simulation. The company produces several cyber wargaming support products including technical testing and environmental build-out automation. A training offering, based on a scenario of an adversary operating inside the network, produces exercises to improve real-time responses against live, multi-stage attacks from external and internal sources.

3.2.5 Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA)

Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA) [Applebaum 2016] is a MITRE-developed technology and an extension of the ATT&CK adversary threat model framework. Its objective is to automate emulation of post-compromise cyber threat behavior to test defenses and develop more effective detection analytics. It provides a capability to use a simulated red team, rather than a live one, by automating the execution of sequences of attacker techniques drawn from ATT&CK using a planning engine. Currently, the framework's intrusion automation is being used to cause effects to files, process, network activity, and system configurations as a basis for testing and improving detection analytics. By using a repeatable orchestration engine and applying different variations of behavioral sequences against an analytic it can prevent detection algorithm over-fitting. It is also being used to test defensive technologies in an automated testbed.

3.3 Exercise Environments and Tools

This section summarizes environments being used to support advanced cyber wargaming exercises. While some may be available for FSS use through a commercial vendor, others are included as examples of environments being used elsewhere for these exercises.

3.3.1 Fort Meade Experiment (FMX)

The Fort Meade Experiment (FMX) environment [MITRE 2012b, Kemmerer 2016] is a MITRE "living laboratory" exercise environment in which a series of red team exercises has been held. In these exercises, live red teams conduct operations against a live corporate network actively defended by a blue team. These iterative exercises proceed as follows. Blue teams deploy sensors to detect adversary activity, red teams attempt to penetrate the defended network, a hotwash session between the two sides is held after the completion of the exercise, and the blue team deploys improvements to their defenses for the next iteration. This work served as the basis, in part, for development of the MITRE ATT&CK Framework.

3.3.2 National Cyber Range

The National Cyber Range (NCR) is a U.S. Department of Defense (DoD) facility that provides a secure and isolated environment to perform training, testing, and evaluation of realistic cybersecurity activities [NCR 2015]. It has four key components: a secure facility, integrated tools for cyber testing, automated tools to configure a testbed with a tailored security architecture, and trained staff to support events. It has the capability to provide testing at classified levels and can host up to four independent tests concurrently.

3.3.3 Lincoln Adaptable Real-Time Information Assurance Testbed (LARIAT)

The Lincoln Adaptable Real-Time Information Assurance Testbed (LARIAT) is a capability created by the Massachusetts Institute of Technology (MIT) Lincoln Laboratory that can generate and run a simulated testbed environment that emulates a network with a large number of virtualized hosts, with associated application software and simulated user activity, including tasks such as web browsing and processing email. The environment allows for evaluation of attacks and defenses at the host and network layers with the capability to emulate Internet connectivity. Originally described in [Rossey 2002], LARIAT has been significantly extended and improved.

3.3.4 SimSpace

SimSpace (https://www.simspace.com) offers an automated tools capability to support operational cyber ranges with an ability to create/re-create, configure, and validate a virtual environment based on an existing infrastructure. The product also provides assessment tools to collect and analyze data during a test event. This produces a repeatable set of infrastructure builds to support control effectiveness measurements.

3.4 Simulations

The following are examples of simulation components that have been developed and used specifically for some form of cyber wargaming.

3.4.1 Analyzing Mission Impacts of Cyber Actions (AMICA)

Analyzing Mission Impacts of Cyber Actions (AMICA) is a prototype cyber simulation system that combines process modeling, discrete-event simulation, graph-based dependency modeling, and dynamic visualization [Noel 2015]. It captures process flows for modeling mission tasks as well as cyber attacker and defender tactics, techniques, and procedures (TTPs). Using a functional model developed in collaboration with DoD operators responsible for a real-world military mission, it was used to model, simulate, and quantify the impact of cyber attacks on the target mission.

3.4.2 Hacknet Labyrinths

Hacknet Labyrinths is a multi-player terminal-based hacking simulator for personal computers (PCs) published under the Steam Gaming platform (http://store.steampowered.com/app/521840). It simulates attack response actions through the use of common forensics and hacker tools, mimicking a Unix-based system. This provides a blue team defensive experience. Scores are derived from successful defense actions. The game is derived from the Hacknet open source project (https://sourceforge.net/projects/hacknet/).

3.5 Adversary Emulation

To conduct cyber wargaming, some method of emulating the activities of the adversary is required. Emulating adversaries accurately requires both a model of the specific capabilities and motivations of the adversary (or class of adversaries) of concern and either a human team or simulation to play the role of the adversary in selecting and conducting attack actions. The former is provided through the use of a specific threat model, along with a set of rules of engagement. A companion report to this one, “Cyber Threat Modeling, Survey, Assessment, and Representative Framework” [Bodeau 2018], provides a threat modeling framework and sample high-level threat model focused on the FSS.

The means of filling the adversary role may vary depending on the level of cyber wargame. In offensive/defensive red-teaming exercises, a human red team is used to play the part of the adversary. These red teams usually consist of individuals who are trained and experienced in live penetration of computer systems. Penetration testers are a good talent pool to draw from, as these individuals have the skills needed to break into systems, establish control and persistence, and move laterally in the fashion of an advanced adversary. Within the realm of penetration testing, different skill sets are available, including infrastructure hacking, web-application hacking, and specialties in compromising and persisting in Windows, Linux, or other platforms. Toolkits used by these red teams include a mix of open source products such as Metasploit, Nmap, and Nessus, as well as commercial products such as CORE Impact, Cobalt Strike, and Burp Suite.

In tabletop cyber wargames, emulation of the adversary can be conducted with less detailed representations of cyber attack steps and does not necessarily require hands-on experience. Adversary behavior can be emulated via white-card actions supplied as part of the exercise scenario, or adversary actions can be selected from a pre-determined vocabulary of simplified adversary actions.

In addition, capabilities are emerging to provide automated adversary emulation based on a more detailed model of adversary tactics and techniques such as MITRE's ATT&CK framework [MITRE 2015]. An example of such a capability is CALDERA (see Section 3.2.5).

3.6 Exercises and Scenarios

The following subsections outline relevant types of exercises and scenarios identified.

3.6.1 Hamilton Series

The Hamilton Alliance Tabletop Exercise (TTX) (https://www.sifma.org/resources/general/cyber-and-operational-resilience-table-top-exercises/) was one of a series of joint U.S. Government – FSS exercises sponsored by the Treasury Department and DHS. Earlier iterations of the Hamilton series focused on incident response to specific attack scenarios and the associated capabilities and processes in the sector. The Hamilton Alliance exercise included FSS firms, the Financial Services Sector Coordinating Council (FSSCC), federal regulators, and DHS. The wargame scenarios were based on information sharing between government components and the private sector. Communications mechanisms at the time of the event were exercised with the objective of improving the efficiency and effectiveness of notifications across privacy and classification boundaries through interfaces such as the Financial Services Information Sharing and Analysis Center (FS-ISAC).

3.6.2 Quantum Dawn Series

The Quantum Dawn series of cyber wargames (http://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-iv/) were tabletop exercises to test incident response, resolution, and coordination processes for the FSS and the individual member institutions faced with a sector-wide cyber attack [Deloitte 2015]. The Quantum Dawn wargames were held by the Securities Industry and Financial Markets Association. The NUARI DECIDE product was used to support automation of the scenario. Participants included many of the large FSS members, FS-ISAC, DHS, law enforcement, and regulatory agencies.

3.6.3 RSA 2016

The Learning Labs portion of the 2016 RSA Conference included an international financial cyber crisis tabletop exercise called "Financial Sector and the Evolving Threat Landscape" [Fox-IT 2016]. This event was designed as a paper-based exercise with a facilitated discussion of a scripted scenario, with planners and players sitting together in one room for the exercise execution.

3.6.4 RSA Singapore 2016

In the Learning Labs portion of the 2016 RSA Conference Asia Pacific and Japan, held in Singapore, Cyber-Monkey was a scenario-based tabletop exercise for executive management to role-play a corporate breach [McCombie 2016]. Constrained to management and public release messaging, it focused on a Security Operations Center (SOC) manager briefing the Chief

Information Officer (CIO), the CIO interacting with the corporate Board, a corporate spokesperson interacting with the media, and the Chief Executive Officer (CEO) appearing before a central government entity.

3.6.5 DHS Cyber Storm Series

The DHS Cyber Storm wargaming series (https://www.dhs.gov/cyber-storm) is sponsored by the DHS Office of Cybersecurity and Communications (CS&C). DHS Cyber Storm wargames are tabletop exercises focused at the national level on incident response processes and preparedness. The exercises are scenario-based and simulate cyber attacks on critical infrastructure elements, including the Domain Name Service and Internet traffic routing, that affect corporate and government systems. Responses are evaluated with a focus on prevention, protection, mitigation, response to, and recovery from incidents. The games are designed to raise awareness of threats, improve information sharing, and improve incident response TTPs.

3.6.6 BSides Las Vegas

BSides Las Vegas (https://www.bsideslv.org**)** is a yearly conference held in conjunction with the Black Hat and DEFCON conferences. One of the activities it features is a technology wargaming event between competing defensive teams. The event includes a red team, blue team, white team, and administrative process. No scenario involving non-technical incident response or management oversight is included; however, the scenario contains system administration tasks for the blue team to complete that are designed to simulate human dual-role tasking similar to corporate organizational practices. Defending blue team members are given system administrative rights to their domain and asked to securely configure their systems while maintaining critical externally-facing services such as web and email. Red team members are provided with hacking tools and systems to launch attacks. Metrics are based on service uptime, avoiding "flags" or files captured, completion of administrative tasks, and the defenders' ability to limit red team penetration, which is measured by the number of beacons successfully planted in defended systems by attackers to phone home to the scoring engine.

The 2017 BSides Las Vegas event included an initial introduction of composite wargaming elements. The concepts of money as a resource constraint and cumulative gaming score were introduced to the technical Red Team / Blue Team exercise. Money could be used by the Blue Team to purchase capabilities that could then be used to improve defenses of their systems infrastructure. Successful defense from Red Team attacks increased the money balance over time. The game objective of the new element leveraged the concept of Return on Investment (ROI). Rules for the 2017 cyber wargame can be found on the Bsides website: (http://prosversusjoes.net/BSidesLV2017ProsVJoesCTFrules.html).

3.6.7 Bank of England Series

The Bank of England has run a series of tabletop cyber wargames for the United Kingdom's financial sector. These include Resilient Shield, held in conjunction with the U.S.[8] in 2015,

[8] https://www.gov.uk/government/news/transatlantic-exercise-to-tackle-cyber-threat

which had no live system involvement, and focused on information sharing and planning. Prior exercises, Waking Shark in 2011 and Waking Shark II[9] in 2013, involved multiple scenarios with simulated attacks.

3.6.8 Capture-the-Flag Events

Capture-the-flag events are live cyber events in which participants are given a challenge to achieve in the target system, such as modifying a file or obtaining privileges. Capture-the-flag events are typically less structured and not based on a mission scenario. These events are held by a wide array of diverse organizations in academic, conference, government, or corporate settings. The following subsections describe a few representative examples.[10]

3.6.8.1 New York University Cyber Security Awareness Week (CSAW) Capture the Flag

The New York University Tandon School of Engineering's Cyber Security Awareness Week (CSAW) games are held yearly and include a Capture the Flag (CTF) competition (http://cyber.nyu.edu). These are unstructured entry-level hacking competitions focused on offensive attacks on vulnerable applications. Metrics are based on captured "flags" or files, with point scales for each. No operational scenario is used to guide activities, and only an administrative white team is used to evaluate and control game play.

3.6.8.2 DEFCON Capture the Flag

A Capture the Flag event is held as part of the DEFCON security conference in Las Vegas each year. This is an offense-defense style game which requires player teams to reverse-engineer custom binaries to identify vulnerabilities and attack them, earning credit for compromising competitors' systems while defending their own. It is a non-scenario format with relatively simple logistics, engineering, and operations work to establish the individual contests in the game, focused on binary reverse engineering, patching, and exploitation. Metrics and scoring are awarded based on completion of the individual challenges, which are not contingent on completion of other tasks.

3.6.8.3 UC Santa Barbara International Capture the Flag

A periodic Capture the Flag event is held by the University of California Santa Barbara using the Security Lab and iCTF Framework (https://github.com/ucsb-seclab/ictf-framework) in a multi-site, multi-team wargame with teams competing independently against each other. It follows the model of typical Blue Team exercises of protecting system services and the files on the systems from capture by opposing players. Scoring is awarded based on captured flags from other teams' systems.

[9] http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf

[10] More examples, and links to toolkits for developing capture-the-flag (CTF) events, can be found at http://resources.infosecinstitute.com/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/#gref

3.7 Portraying Defensive Capabilities

Extensive work is in progress across the community to develop improved situational awareness / situational understanding capabilities for detecting post-compromise activity on networks and in systems. Commercial and open source projects continue to progress toward a more mature capability. These often leverage previous work with log and activity consolidation, as well as supporting development of newer cyber-related sensors based on an analytic ontology to support cyber defensive responses to events.

Developing a common, reusable repository of analytics for detection against known attack vectors and supporting more rapid reaction to changing vectors is a common theme across the industry.

3.7.1 Cyber Analytic Repository (CAR)

Building on the ATT&CK framework, a Cyber Analytics Repository (CAR) to support cyber defenders has been developed (https://car.mitre.org). For each analytic, this repository includes:

- hypothesis explaining the idea behind the analytic
- operational context (e.g., host, network, process, external)
- cross references to the ATT&CK framework
- pseudocode description of potential implementation
- identification of what sensor information is needed for use of the analytic

An ontology such as that embedded in CAR could provide a possible basis for creating a modeled representation of the operation of sensors and analytics in a cyber wargame, providing more fidelity and realism than white-carded events, without actually running the sensors and analytics in a testbed as part of the game.

4 Applying Composite Cyber Wargaming to Financial Services and Other Sectors

The practice of cyber wargaming has been adapted from other mission-based operations such as exercises conducted by the DoD to model and simulate battlefield defensive and offensive operations. It supports development of TTPs by identifying weak or ill-defined areas of operational integrity. Adaptation of wargaming to cyber has been predominantly focused on either scenario-based tabletop processes or technology-based defensive and offensive tool utilization.

The progression of effectiveness for both adaptations has limitations based on their focus and context. An exercise based on human processes and interactions leaves undefined – or highly abstracts and simplifies – the elements of severity of technology attacks and variability of impacts. Technology exercises like red-teaming lack an element of human response to events and the variability of business impact due to disruptions of specific applications, associated business functions, and inter-entity dependencies.

4.1 Cyber Wargaming Objectives

As cyber protection continues to mature, areas need to be identified to support development of more sophisticated modeling and simulation scenarios. The merging of the two existing methods via composite cyber wargaming could identify impact to operational integrity that would result from realistic interaction between technology failure modes and needed realignment of business area functions (also referred to as mission).

For example, the collapse of the World Trade Center towers had an operational effect for all the FSS institutions, including those that were located in New York City and others that used the services of institutions such as the Stock Exchange or Federal Reserve. The severity of the impact depended largely on two factors related to operations based in lower Manhattan:

- Network connectivity paths between the FSS institutions, the Federal Reserve, and the Stock Exchange were routed through three telecommunications provider buildings;
- Power to data centers and office buildings was sourced from multiple distribution centers.

As the events of the day unfolded, decisions on implementation of operational contingency plans and closing or substitution of business execution were made. The scenarios of the event were in some instances anticipated, while others required adaptation and adjustments to operational processes.

Objectives to continue to improve the realism, training effectiveness, and operational dependency insights of cyber wargaming for each of the cyber constituencies' needs are outlined below.

4.1.1 National Level Objectives

The national mission to protect critical infrastructure against the impact of successful cyber attack requires effective event response and threat intelligence. DHS, along with commercial

ventures, serves as a cross-sector operational facilitator of intelligence, event notification, threat vector identification (e.g., actor, motivation, target), and impact assessment.

Consideration of objectives for improving wargaming should include identification of improvements to timeliness and effectiveness to support:

- Communication of active threats, event notification, and operational mitigation tactics
- Coordination of sector-level and cross-sector efforts to address significant threats common to the member institutions
- Development of improved mitigation technology for use by constituent institutions to address gaps and weaknesses in threat mitigation.
- Identification of scenarios that consider national, sector-level, and multi-party risk mitigation TTPs and technology gaps.

4.1.2 Sector-Level Objectives

With the objective of developing new risk and threat models to support cyber defense improvements, this report is focused on the FSS. However, while the specifics will vary, the general approaches and concepts in the report apply equally to other sectors and industries.

Many of the larger FSS institutions have adopted risk management and incident management practices that can serve as a baseline for other critical infrastructure sectors, as well as provide usable best practices and measures for other institutions within the sector. Continued adoption by midsize, smaller, and dependent utility institutions also presents areas for continued improvement. Such institutions could benefit by:

- sharing best-in-class technologies and processes such as those exhibited in FS-ISAC's implementation of Structured Threat Information eXpression (STIX) [OASIS 2016] and related TTPs
- participating in tabletop wargaming exercises such as the Hamilton series and other models
- deploying red team testing
- conveying requirements for remediation and improvements as customers to major vendors of cyber products

Further efforts remain to improve propagation of cyber technology and TTPs to others and to continue to develop the starting baseline described above. Objectives for additional effort should include:

- stronger intelligence quality and sharing mechanisms
- improved adversarial attribution and actionable counter measures
- better technology transfer across the sector(s), and

- introduction of comprehensive learning of event management actions and impact assessment

4.1.3 Individual Institution Objectives

Although many FSS institutions have mature operational cyber programs, they could remain at risk in various areas to unidentified or unmitigated threat vectors. Also, smaller institutions may need to incorporate lessons learned, technology research, and systemic risk solutions from the larger sector members to improve their ability to protect themselves and reduce upstream risk to their larger partners.

Areas for potential inclusion are:

- Third parties such as power suppliers, telecommunications providers, operating consumables (e.g., paper, ink, facility supplies), and subordinate transaction generation companies
- Market utilities such as Society for Worldwide Interbank Financial Telecommunication (SWIFT), FedWire, New York Stock Exchange (NYSE), and NASDAQ
- Interdependence of partner institutions for lending (e.g., Fed Funds, Discount Window)
- Interdependence of system application functions (e.g., Demand Deposit, Brokerage, Funds Exchange, Funds Transfer)
- Threat anticipation, attack vector adaptation, long-term persistence

4.1.4 Public

The role of the consumer or customer of financial services and other critical services is a key component of any event scenario that may become visible outside an institution. An incident could prevent the institution from participating in transactions or have an impact on continued business interactions due to the failure to execute in a timely fashion, the appearance of being out of control, or the perception of a direct impact to the public. Process errors, inappropriate public communication, and the loss of technology availability can quickly drive financial losses and cause an erosion of trust in the financial system.

Areas of concern would include:

- Perception of loss of trust in transaction integrity and in ability to fulfill commitments
- Reliance on endpoint and application integrity by all parties to transactions
- Legal action against multiple institutions
- Civil panic or unrest
- Law enforcement support and capacity

4.1.5 Technology

Financial services transaction flows have become dependent upon technology, with very few viable manual alternatives remaining. The shift to a cashless transaction base has made the basic distribution of consumables for everyday life in the U.S. heavily dependent on an electronic transfer of value between supplier and consumers of commodities at all economic levels. Even the most disadvantaged members of the population are provided Electronic Benefits Transfer (EBT) cards for food stamps, welfare payments, and emergency payments (e.g., by the Federal Emergency Management Agency [FEMA]).

While the associated infrastructure is resilient to a level of fraud and failure, systemic risk to broad-based failures remains a significant threat. A valid scenario such as a failure of a card transaction authorizer like VISA demonstrates a large-scale outage that would be specific to an individual card issuer. Even a cascading failure from a technology vendor with a significant market share (e.g., McAfee, Microsoft, Apple IOS, or Cisco) could undermine transaction availability and integrity.

Possible areas to consider for scenario inclusion would be:

- Gap assessments of specific products
- Product strategies and lifecycle management processes
- Diversification of technology utilization
- Rapid detection and response to cascading failure modes; autonomic redundancy and execution throttles
- Single or minimal sourcing alternatives

4.2 Composite Model Rationale and Measures of Success

While the two traditional types of cyber wargaming, tabletop and red teaming, are well established, creating a composite model that bridges the gap between the two extremes will yield additional benefits for the betterment of the entire sector. While classic hands-on experimentation can yield high-fidelity understanding of cyber risks and the technology issues or gaps, conducting such exercises is costly and time consuming. By contrast, while tabletop exercises are much less costly or complicated, they look at the world through a very macroscopic lens that often does not take technology or cyber risks into consideration.

By creating a composite exercise that borrows from both extremes, it should be possible to glean additional insight regarding technology capabilities or gaps and inherent cyber risks in engineering and architectural choices, without the extreme cost and effort of detailed technical experimentation.

It should be possible to create an emulated environment that mimics a typical enterprise defensive suite to allow simulations of attack and defense. This will support the execution of different scenarios to try to determine the effects of technologies used in protecting an environment (i.e., firewalls, intrusion detection systems, antivirus, etc.) for providing detection

of and response actions to an incident, through their effectiveness in handling offensive actions in the simulation.

As an added benefit, such simulations could provide training to mid-level managers and technicians who might otherwise have insufficient experience when confronted with a real cyber event in a crisis situation by placing them in a scenario to observe and respond to a realistic threat being executed against a live or simulated infrastructure.

Business operations rely on supporting technology platforms and their ability to maintain confidentiality, integrity, and availability at an ever-increasing pace. Cyber attacks provide a path to disrupt the execution of business transactions at all levels through direct interference with the effectiveness of technology and operational controls.

Current wargaming methods stratify between operational processes and technology-based defenses. Given their symmetric reliance and the need to defend both in parallel, variations in a composite set of gaming scenarios are needed. The objectives should be to generate teachable events in the wargaming exercises for business executives, mid-level business operations management, technology management, and their respective operational and engineering teams.

Utilizing a broader integration of these capabilities to test and refine clear and effective response processes, communication channels, and technical reaction options will improve the outcome of real events. Also, repetitive practice of a mix of operational components drives collaborative solutions and better understanding of each team's role.

For a composite cyber wargaming exercise to be successful, it is important to identify the metrics that will be used to measure how well the participants were able to achieve the defined objectives. This provides a series of benefits, including identifying and quantifying areas needing improvement on the part of the participants, determining the effectiveness of technology in the defense presented, and identifying opportunities for improving future composite exercises.

Depending upon the scenario and its objectives, one or more of the types of metrics shown in Table 2 may be appropriate to implement in a composite cyber wargaming exercise.

Table 2. Defender Effectiveness Measures

Metric	Description	Measurements
Minimizing Impact to Business Operations	Actions on the part of defenders that are attempting to respond to an intrusion can have an impact on Business as Usual (BAU) activities.	**Service Uptime** – for the duration of the exercise, what % of time are the business services available? **Service Integrity** – for the duration of the exercise, what % of the time are the integrities of the business services compromised?
Identifying Hostile Activity	Whether the defenders can determine that the defensive perimeter has been breached and hostile activity is underway.	**Compromised Systems** – can the defenders identify which systems are compromised? **Command and Control (C2) Channels** – can the defenders identify management communications through their perimeter?
Identifying Exfiltration	Whether the defenders can determine that critical data has been obtained by hostile actors and is being staged and/or exfiltrated	**Staging of Data** – can the defenders identify where the data is being staged for exfiltration? **Data Transmission** – can the defenders identify the exfiltration of compromised data?

Metric	Description	Measurements
Remediation of Compromise	Whether the defenders can remediate compromised systems to expel hostile actors.	**Compromised Systems** – how many systems can the defenders reclaim control of? **Vulnerabilities Closed** – how many vulnerabilities can the defenders close in systems to prevent new compromises?

Attacker Effectiveness Measures, shown in Table 3, can be used as an additional means to assess defenders, but are primarily for assessing the effectiveness of defensive technology.

Table 3. Attacker Effectiveness Measures

Metric	Description	Measurements
Vulnerabilities Discovered	Whether or not the hostile actor is able to identify any vulnerabilities that can lead to a breach.	**Vulnerabilities Discovered** – how many vulnerabilities is the hostile actor able to discover?
Systems Compromised	Whether or not the hostile actor is able to breach the perimeter and attain persistence, to what scale and severity.	**Compromised Systems** – how many systems can the hostile actors gain control of? **Level of Criticality?** – how many critical systems is the hostile actor able to gain control of?
Data Obtained	Whether the hostile actor is able to get access to and control of critical data protected by the defenders.	**Access Gained** –was access to the data obtained by the hostile actor? **Data Exfiltrated** – was data exfiltrated by the hostile actor?
Stealth	Whether the hostile actor was able to achieve their objectives in a stealthy manner.	**Time Before Detection** – how long was the adversary able to operate undetected?
Downtime Achieved	In the case of a denial of service exercise, whether the hostile actor was able to deny access to the defended system.	**Time of Outage** – for the duration of the exercise, how long was the denial of service effective?

4.2.1 Spectrum of Wargame Levels

Table 4 illustrates the broad range of possibilities for implementing wargames at different levels. This table shows the key aspects of each level of cyber wargaming, from tabletop to red-team exercises, with an outline of what composite wargame events might entail. To bring cyber wargaming to the next level, each scenario would seek to build on interaction levels, event complexity, needed participant skills, and targeted result areas of the exercise.

Table 4. Integration Levels

Scenario elements	Model Type	Approach	Participants	Events or Behavior Examples	Desired Result
Public communications Constituency communications	Tabletop: White card	Verbal walk through of a planned scenario	Management teams: executive, business, technical	Develop public message content Release to media, and field questions and answers Brief Board, senior executives Communicate to internal workforce	Manage cyber event; review decisional choices; develop after-action follow-ups; train participants
Failure due to technical architecture choices Reactive course of action Internal/external communications	Tabletop: White card Variable impact from technical or utility dependency	Develop action plan with interaction based on specific functional failures Decisions on operational actions based on outage and dependencies	Management teams: executive, business, technical, operations Technical: SOC; system administrators	React to technical active attack scenario Simple impact assessment based on a technical component (e.g., Windows vs. Linux, Cisco vs. Juniper) Course of action (COA) development based on time to repair and impact to business Internal and external communications and intelligence	Manage broader cyber event impact; exercise possible technical response actions; event notification/ messaging
Significant product / technology vulnerability Active exploitation Detect and remediate	Tabletop: White card for event Specific vulnerability being exploited Business impact assessment	Drive event remediation of technology attack Cross-sector and cross-business and operations entities within firm Drive efficient remediation methods	Management teams: executive, business, technical, operations Technical: SOC; situation awareness business operations IT operations	React to technical active attack scenario Impact assessment based on technical component and business function (mission mapping) COA development based on time to repair and impact to business Internal and external communications and intelligence	Event management to cross-sector or sector level impact Measure response capability and strategy across business and sector lines; COA development; response timelines

Scenario elements	Model Type	Approach	Participants	Events or Behavior Examples	Desired Result
Introduce technical architecture derived from testing with variability by firm	Composite: Tabletop response with variability driven by deployed technology Analysis of technical threat vector against current tools and architectures	Tabletop a scenario against specific threat vectors from the threat model Analyze firm's deployed security posture for unmitigated technical risk Determine possible alternative controls and technologies Develop cost and operational effective response(s)	Management: business, IT, operations, cyber Technical: application development, SOC, cyber engineering, systems and network engineering	React to technical active attack scenario Impact assessment based on technical component and business function (mission mapping) COA development based on time to repair and impact to business Initiate attack and defense activities Respond to successful breach and assess business impact Estimate recovery method and time-window options by firm, and work across firms or business dependent areas	Leverage product evaluation(s) against selection criteria and threat matrix Drive product and architecture improvements Exercise priority setting for response actions Develop context for improvements and update reference data
Model institution elements in common range Execute active offensive and defensive actions by exercise red team and institution's blue team	Composite: Active offensive and defensive in a cyber range Scoped to common business function technology platform	Tabletop for business communications; operational stability; impact assessment Active attack against range systems with defensive and detective response COA identification for operational integrity	Management: business, operations, cyber Technical: application development (as needed), SOC, cyber response (Computer Emergency Response Team [CERT]) penetration testers	Identify business function(s) scope and model support technology in cyber range Initiate attack and defense activities Respond to successful breach and assess business impact Estimate recovery method and time-window options by firm, and work across firms or business dependent areas Develop contingency COA to fight through attack to deliver optimum sector and/or institution operational status	Exercise priority setting for response actions Develop context for improvements, and update reference data A post-game hotwash session between red and blue teams to facilitate learning on both sides

Scenario elements	Model Type	Approach	Participants	Events or Behavior Examples	Desired Result
Red vs. Blue Capture the Flag (CTF)	Active offense and defense in a cyber range	Live offense and defense exercise in a contained network of target computers	Trained penetration testers Defensive cyber personnel	Attack defended systems to penetrate, gain control, persist, and perform actions on objectives (e.g., steal data) Defend systems by hardening environment, identifying compromises, and remediating affected systems.	Observe live, real-time offense and defense to learn the value of offensive and defensive technologies and TTPs. A post-game hotwash session between red and blue teams to facilitate learning on both sides
Red Teaming against production staging areas (e.g., quality assurance [QA])	Hacking tools and advisory tactics Monitoring of detection tools	Live hacking using penetration-testing methods Defensive observation of attack activity	Trained penetration testers SOC	Active hacking team (red) attacking production systems and infrastructure in a controlled test Identification of activity and methods (ATT&CK)	Discovery of technical vulnerabilities, architectural flaws Measuring detection effectiveness
Direct attack of production environment with defensive participation	Hacking tools and advisory tactics Monitoring of detection tools	Live hacking using penetration-testing methods Defensive observation of attack activity	Trained penetration testers SOC	Active hacking team (red) attacking production systems and infrastructure in a controlled test. Identification of activity and methods (ATT&CK)	Discovery of technical vulnerabilities, architectural flaws Measuring detection effectiveness
Direct attack of production environment	Hacking tools and adversary tactics	Live hacking using penetration-testing methods	Trained penetration testers	Active hacking team (red) attacking production systems and infrastructure in a controlled test.	Discovery of technical vulnerabilities, architectural flaws

4.2.2 Scenario Development

Many different scenarios could be developed and implemented in composite cyber wargaming exercises to achieve the purpose of identifying effectiveness of institutions' processes, personnel, and technology and areas for improvement. Using elements from the integration levels against threat vectors from a threat framework, a set of outcomes could be developed to extend the game-play to more advanced adversary TTPs and attack patterns. With ongoing updates to the threat model, this could be refined over time as new threats are identified and their behaviors categorized. Using the framework and high-level threat model in the companion "Cyber Threat

Modeling Survey, Assessment, and Representative Framework" [Bodeau 2018] as a starting point for building a scenario, the following are several examples of defender goals which could motivate a variety of scenario steps at multiple levels.

- Identifying compromise of defended systems by sophisticated threat actors
- Identifying compromise of defended systems by self-propagating malware
- Actively defending against sophisticated threat actors
- Remediating defended systems affected by self-propagating malware
- Remediating defended systems affected by ransomware
- Defending against distributed denial of service attacks

4.2.3 Existing Capabilities and Gaps

Existing capabilities for cyber wargaming include platforms, exercises, and tools that have followed a tabletop model. Such capabilities support TTPs that are management and operational process-based and executed against pre-built game scenarios. These are best illustrated by the Hamilton, Quantum Dawn, RSA 2016, RSA Singapore 2016, and DHS events (Sections 3.6.1 through 3.6.5).

Technical wargaming exercises, in contrast, have focused on derivatives of penetration-testing assessment methodologies developed to support operational readiness processes for the DoD and others. This approach has been adopted by the cybersecurity industry and adapted to common tools such as Metasploit, Nessus, and Nmap. The mixture of offensive and defensive roles has been added, as well as elements of game play such as capture-the-flag objectives, to extend the events to a more realistic cyber attack-and-defend scenario. These are best exemplified by the BSides, DEFCON, and academic capture-the-flag events.

Both of these constructs drive a test of defined dependencies and TTPs, as well as having educational practice benefits. The technical elements provide an assessment of the security of the software and configurations as a measure of the overall protection. The integration of elements that leverage both of the models should drive improvements in understanding of technological dependence at a level not available today.

The survey found technologies and building blocks applicable to cyber wargaming in some areas and gaps in others.

- **Frameworks and models:** The Wargame Construction Kit was designed for military wargames. While an analogous capability could be developed for cyber wargames, it is not directly applicable to cyber wargames in its current form.
- **Platforms:** The platforms identified provide several possibilities for composite cyber wargaming, ranging from a graphical user interface (GUI) for immersing tabletop cyber wargame participants in a situational context to a board game resembling a military wargame but populated with white cards for technically realistic cyber attack techniques

and defense actions, to toolkits for constructing emulated enterprise architectures with cybersecurity instrumentation for testbed-based experimentation or exercises.

- **Exercise environments and tools:** The exercise environments and tools identified include examples of a several types of environments or tools. One is a "living lab" testbed that is heavily instrumented and available for emulated cyber attacks while simultaneously supporting real-world operational users. Another is a cyber range designed for set-up, execution, and tear-down of large-scale test/exercise configurations including real and emulated systems. Last are tools for generating traffic and workloads to run on a network environment representing the business users and activities on the system during exercises.
- **Simulations:** Cybersecurity simulations identified are early examples of simulations representing cyber actions and impacts that could eventually be incorporated into cyber wargames.
- **Exercises and scenarios:** The cyber wargames and red-teaming exercises identified mainly represent either the high-level tabletop type of wargame focused on business impacts and coordination or the detailed, hands-on red-teaming type of wargame against a generic or hypothetical network architecture and with a technology-focused objective.

4.3 Technology Mapping to Composite Cyber Wargaming Elements

Supporting technology for composite wargaming events remains incomplete. Gaps remain for both scenario execution support and an orchestration of emulated attacks and responses. Recent events such as the Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge and ongoing defensive games like the National Collegiate Cyber Defense Competition continually improve live and emulated tools and tactics.

Work in this emerging area is continuing, and some recent research has been active within the Navy and Army laboratories[11] of the DoD. However, these remain in progress and are not fully scoped to the differing layers of possible technology integration in wargaming exercises.

Table 5 shows examples of how capabilities of the surveyed products currently available to the FSS could be used to provide the abstract elements needed to conduct a cyber wargame[12]. Each element could be provided through a range of approaches from scripted and largely manual, to simulated, to simply having live participants operate in a live systems environment.

[11] Navy, Defense Technical Information Center, Orchestrated Simulation through Modeling (OSM), NAVSEA; Army: 12th International Conference on Cyber Warfare and Security, 2017 Proceedings, Cyber Wargaming on SCADA Systems (January 2017), US Army Research Laboratory, Ed Colbert, et al.

[12] In cells left blank in the table, none of the surveyed products would readily provide the element for that type of wargaming approach. For instance, capabilities to support some elements of a simulated approach are at a very early stage and would need to be developed further.

Table 5. Alternatives for Implementing Wargame Elements

Wargame elements	Scripted (Card/ Tabletop)	Process Based Multipath	Simulated	Emulated	Live Exercise
Attack Step Selection	Script	Cyber Gym Maelstrom		BRAWL[13] Rapid7 (Metasploit)	Metasploit Human red team
Defense Step Selection	Script	Cyber Gym Maelstrom	CALDERA		Human blue team
State Change Evaluation / Execution	Disclose result	DECIDE			
Testbed	SimSpace	DECIDE		LARIAT KALI Linux BRAWL	NCR BSides
Attack Vocabulary	ATT&CK (Windows)	ATT&CK (Windows)	ATT&CK (Windows)		Armitage[14]
Defense Vocabulary		Maelstrom	STIX CAR CAPEC CybOX[15] CALDERA		
System	N/A	N/A		LARIAT KALI Linux	Real hardware and application execution

[13] See [MITRE 2017].

[14] Strategic Cyber**,** Raphael Mudge, Armitage, Metasploit orchestrator, http://www.fastandeasyhacking.com

[15] See [MITRE 2012].

5 Enabling Capabilities for Testing and Wargaming

To accomplish an offense-on-defense exercise, the reuse of actual attack scenarios on modeled systems and applications would enhance the simulation by reflecting the variability of actual threat events. Utilizing the attack vectors, adversarial TTPs, and targeted technology captured in the STIX/Trusted Automated eXchange of Indicator Information (TAXII) ontology could produce a set of replayable testing capabilities. Programmed use of an attack platform, such as Nessus or Metasploit, would provide a repeatable result for a targeted piece of technology supporting the business function of the wargaming scenarios.

Defining a set of language elements to support development of attack automation against specific mission elements may include:

- Transformation of the STIX ontology to a usable set of replayable attack constructs, usable courses of action (COAs), and associated technology targets.
- Execution language for orchestration of a test harness for automated testing of controls, for instance using CALDERA, as described in Section 3.2.5.
- Definition of scope and hierarchical chaining potential for advancing a campaign
- Measures and messaging to support COA adjustments, eventually as an autonomous response.
- Ingest of new STIX-reported TTPs to capture changes to attack vector models and produce updated attack execution vectors.
- Enumeration of detection methods and mitigating responses
- Reporting to support metrics generation over time

5.1 Game Structure

The following section outlines a structure that could be used to construct and operate a composite wargame.

5.1.1 Process Overview

As described in Section 2.6, cyber wargaming can be represented via an abstract reference model capturing its fundamental elements, including the required participants, processes, and data resources. These elements can be provided through a range of means. For instance, the selection of attack actions can be done by a human team emulating an adversary, by a sophisticated artificial intelligence planner, or by something as simple as a random selection from a pre-defined set of actions. Nevertheless, each element must be present in some form.

Utilizing red, blue, and white teams to support integration of responsibilities for execution of composite wargaming scenarios, an initial example of catalogs of attack actions, business disruption, application / system / network deployment, defensive playbooks, and COA options has been developed. Elements are then selected to build a sample wargame exercise, identify

existing execution platforms, and provide some guidance on automation to support an ongoing effort to engage across the FSS. Ongoing testing, evaluation of results, and updates to supporting effectiveness data could drive gap closures and help close the loop on improved modeling of potential cross-sector impacting events.

5.1.2 Adversary Attack Options

An important aspect of cyber wargames is what options are available to the parties playing the part of the adversary. Aside from their preparations to keep adversaries at bay or respond, defenders tend to be reactive once a breach has occurred. The following are examples of scenario-building attack actions that are based on known events in the FSS. While focused on the FSS, many of these examples are ubiquitous and often apply to all sectors.

In order to deal with the change in threat vectors over time, a process to extract event data from systems such as STIX/TAXII can be used. For a wargaming exercise, a combination of these options can be used as unfolding steps in a modeled scenario.

5.1.2.1 Failure to Protect Data

- Unauthorized Wireless Access Points - An official visitor operates his laptop or personal digital assistant (PDA) in ad-hoc mode while simultaneously connected to the company's wired local area network (LAN).
- Connection of unauthorized equipment to the internal network, Connection of compromised system to the internal network – Attacker gains access to the administrative functions of a home router with ports 21, 23, and 80 open. The attacker can then port forward, sending traffic directly to each machine.
- Connection of compromised system to the internal network – When using a virtual private network (VPN), a third-party program (e.g., iTunes or Skype) "phones home" during a user's session and provides a log without the user's knowledge.
- Connection of compromised system to the VPN.
- Connection of compromised device to internal host (e.g., universal service bus [USB]) – An employee connects a malware-infiltrated USB memory stick into his/her networked computer intending to simply transfer files from the work computer to a home computer to continue work over the weekend, but the network gets infected with the malware.
- Failure to retain data according to policy:
    - Over-retention - Companies retain more records than necessary, exposing themselves to increased responsibility for maintaining and protecting unneeded, but still sensitive, data. Keeping data and documents longer than necessary hurts efficiency, increases discovery costs, and raises the risk of liability.
    - Under-retention – Premature disposal of records may violate legal retention obligations and can result in fines and company reputational damage.

5.1.2.2 Confidentiality Breach

- Improper disposal of persistent information
  - Paper – paper documents, some containing sensitive company information and/or personally identifiable information (PII), are simply discarded in ordinary wastepaper baskets, exposing valuable information.
  - Magnetic Media – Although sensitive files on magnetic media are deleted before disposal, the delete function merely designates the space as available; it does not make the data irretrievable.
  - Removable media (CD-ROM, tape).
  - Photocopiers – modern photocopiers scan and store documents in memory. Unless copier hard drives are wiped clean, sensitive information could remain in storage and susceptible to compromise when copiers are returned to leasing companies.
  - Hard drives – hard drives are returned to leasing agents without proper wiping/sanitizing.
- Automated Teller Machines (ATMs) – card-reading skimmers installed on the mag stripe reader slot to capture card information or data, and personal identification numbers (PINs) obtained by secret cameras and/or shoulder-surfing.
- Transmission of internal data in a non-approved transport – use of internal email to transfer documents containing sensitive information and not encrypted or password-protected per company policies.
- Release of PII – transmission of unencrypted PII information within an email, document, or other electronic format from a company network to a personal email account, even if the PII only pertains to the person transmitting the information.
- Release of Protected Health Information (PHI).
- Release of Merger and Acquisition (M&A) plans – transmission of non-public M&A plans from a network to a personal email or other network without encryption or password protection.
- Release of intellectual property or trade secrets – transmission of files containing intellectual property or trade secrets from a network to a personal email account or other network without encryption or password protection.
- Exporting internal data to non-managed assets – Using non-managed assets (e.g., a personal thumb drive) as a backup storage device for sensitive company data files without encryption/password protection.
- Third-party cloud service, (e.g., Gmail / Yahoo / backup service) – utilizing cloud service providers to back up sensitive company data files without encryption. Relying on cloud as a complete backup solution, not taking into account that most cloud storage services do not support file version control (i.e., if someone overwrites a file, it could be difficult to recover the original).

- Employee-owned hardware (USB / smartphone / printer) – Failure of a company to establish firm Bring Your Own Device (BYOD) policies (e.g., defining which employees can use their own devices, the types of devices they can use, and which applications and data they can use or save on their devices), thereby increasing the company's risks and its network's susceptibility to viruses, malware, and security breaches.
- Data Protection
  - Compromise of encrypted materials – loss of an encrypted USB storage device, laptop or other encrypted electronic device; leaving a terminal logged on when unattended.
  - Compromise of encryption keys – using encryption keys that are too weak to protect data, allowing attackers to easily decrypt messages and steal data.

5.1.2.3 Subversion of Integrity

- Fraudulent transactions – Using coercion and/or shoulder surfing, obtaining access credentials to a wire transfer system, allowing the attacker to bypass multi-person authentication and enter fraudulent wire transfer orders.
- Unauthorized money transfer – Either through computer compromise or social engineering, moving money illegally from the legitimate owner to another account.
- Unauthorized account creation – Through an automated capability, creating unauthorized accounts that persist until detected and removed.
- Alteration of data.
- Malicious data destruction – unauthorized installation of malicious code that destroys data or holds data hostage (ransomware). Such code typically enters the network via a social engineering attack and an employee clicking on a malicious link.
- Theft of users' credentials – Stealing credentials through shoulder-surfing; credential residue during automated deployments: failure to clear out critical files (e.g., sysprep.inf, sysprep.xml, and unattend.xml files), which may hold either plain text or base64-encoded plain-text administrative credentials. When sessions are established in Windows, a reference-counted object is created to maintain the session. Stale sessions still have a handle to that credential in memory for the lifetime of the connection and could keep it indefinitely, at least until the computer is restarted, exposing it to continued risk. Ending a Remote Desktop Protocol (RDP) session by merely closing the application rather than by logging off does not remove the login credential from memory.

5.1.3 Business Functions

A key aspect of composite wargames is the implementation of business functions alongside the technical components of the simulation. In order to run a successful event, the business functions of the sector / industry in question should be examined and modeled so that impacts to these can be appropriately depicted during the course of the event.

Continuing with the example of the FSS, primary business functions are supported by multiple institutions. This may hold true for other sectors as well, particularly those with large, multinational conglomerates. Many transactional elements are dependent on successful completion of portions of the transaction flow by different institutions to ensure accurate and successful completion. This includes:

- Central Bank – Oversees/regulates the operations of commercial banks and implements monetary policy. Supports inter-bank funds transfer of member banks.
- Depository Financial Institutions - Banks that work with consumers and businesses and provide bank services to the general public
  - Commercial Banks
  - National Banks
  - Regional Banks
  - Community Banks
- Non-Bank Financial Institutions – Financial institutions other than banks that also work with consumers and businesses to provide bank services to the general public
  - Credit Unions
  - Savings & Loans (Thrifts)
  - Mutual Savings Banks
  - Internet Banks
- Lending Companies – Companies that typically specialize in making personal loans to less-credit-worthy individuals who cannot qualify for loans through normal banking channels
- Mortgage Companies – Companies engaged in the business of originating/funding residential or commercial mortgages
- Non-depository Institutions – Financial institutions whose primary business is not to take deposits and make loans but to provide other financial services to consumers and businesses
  - Insurance companies
  - Pension funds
  - Finance companies
  - Mutual funds.
  - Brokerage Firms

When designing composite wargaming scenarios, incorporation of process hand-offs as a point of cross-sector risk should be part of the objectives of the exercise. For example, funds transfers to settle inter-bank transactions for community banks or credit unions require an intermediary

member bank for the transaction. Failures in a single application supporting a national bank will have a cascading failure for other FSS institutions. Organizations building composite wargaming exercises should consider their own business processes along similar lines for modeling in the event.

5.1.4 System and Application Mapping

Pre-work for a composite wargame can include surveys of the technology platforms in use at each institution that would be needed to support the business functions being impacted by the developed scenario, as well as the deployed security products in the environment. This information would be mapped to the attack vectors in the scenario to determine vulnerability to each institution's platforms. The survey would be tailored to each scenario and would draw from common commercial technology deployment areas, for example:

- Operating Systems:
  - Windows Server (version)
  - Windows Desktop (version)
  - Apple Desktop (version)
  - Linux Server
  - Solaris Server
  - IBM-MVS
- Asset Ownership
  - Company owned
  - Bring Your Own Device (BYOD)
- Server and Endpoint Applications Commercial Off-the-Shelf (COTS):
  - Microsoft Office
  - Microsoft Exchange Server
  - Apache Webserver
  - IIS Webserver
  - IBM Tivoli
- Business Developed Applications
- Languages
  - Java
  - JavaScript
  - C++
  - C#

  - Microsoft .NET
- Databases and Messaging
  - Oracle
  - Microsoft SQL
  - MySQL
  - IBM MQ Series
  - Amazon Simple Queue
  - TIBCO

5.1.5 Product Threat Mitigation Evaluation

As part of previous HSSEDI work for the NGCI Apex project, an analysis methodology was developed to support technology foraging and product effectiveness assessments.

Updates to operational test and evaluation elements through the composite wargaming exercises would provide result data to support evaluation criteria and provide additional fidelity to product scoring for mitigation effectiveness.

A conceptual methodology to score products against a set of weighted criteria of capabilities, such as that depicted in Table 6, from the earlier work, can be used as an ongoing set of measures. When mapped against control requirement areas, such as network anomaly detection or system intrusion detection, for example, a set of testing results of individual products can be documented. Coupled with ongoing threat updates, a set of gaps can be derived.

Table 6. Product Survey Example

Network-Detect				
Category	**Capability**	**Weight**	**Data**	**Score**
Detection	Signature-Based	1		0
	Behavior-Based	1		0
	Statistical-Based	1		0
	at Line Speed	1		0
	Intrusion Detection	1	1	1
	Intrusion Prevention	1		0
	DDoS	1	1	1
	E-Mail Gateway	1		0
	Malware/Virus	1		0
Sensor Support	802.3 (Ethernet)	1	1	1
	802.11 (WIFI)	1		0
	802.15 (PAN)	1		0
	Full-Packet Capture	1		0
Flow Data	Cisco Netflow	1	1	1
	Argus	1	1	1
	YAF	1	1	1
Standards Support	SNMPv2	1	1	1
	SNMPv3	1	1	1

Network-Detect				
Category	**Capability**	**Weight**	**Data**	**Score**
	IPv6	1	1	1
	Protocol Parsing	1	1	1
	DNS	1	1	1
	SMTP	1		0
	STIX	1	1	1
	TAXII	1	1	1
	CybOX	1	1	1
Analysis	Off-Line Analysis	1	1	1
	Encrypted Traffic	1		0
	Honeypot/Honeynet/Honeyclient	1		0
	Integrated Analytics	1	1	1
	3rd-Party Tool Integration	1	1	1
	Metadata Analysis	1	1	1
		Score		18

5.1.6 Defensive Capabilities

To support improved event detection and timely response to minimize impact, an evaluation of effects caused by the computed business impact is determined. The result is derived for the deployed tools, their ability to drive effective event analytics, and available countermeasures in the progression of the cyber kill chain or cyber attack lifecycle. This is manifested in network and host-level detection, behavior analytics post-exploit, and effective, timely response actions.

5.1.6.1 Detection Tools

Deployed network and host detection tools remain a significant defensive mitigation of most attack methods from both low and medium threat actors. Available commercial products, such as FireEye, Bro, and Splunk, and research work by Sandia Labs, SEI/CERT, Oak Ridge National Labs, DHS, and DoD, continue to enhance the traditional capabilities. These are further enhanced with extended functionality such as sandboxing and honeypot technologies, scripting, and integration with anti-phishing capabilities.

Using data obtained through product testing and evaluations and through analysis of events from platforms such as STIX, an effectiveness value derived as in Table 7 can be used as part of the effect of an attack action in a composite scenario.

Table 7. Use of Effectiveness Values

Category	Capability	Weight	Data	Score
Network Detection	Signature-Based	1	1	1
	Behavior-Based	1	1	1
	Statistical-Based	1		0
	at Line Speed	1	1	1
	Intrusion Detection	1	1	1

Category	Capability	Weight	Data	Score
	Intrusion Prevention	1	1	1
	DDoS	1	1	1
	E-Mail Gateway	1	1	1
	Malware/Virus	1	1	1

5.1.6.2 Analytics

Effective cyber analytics have become a focus of research as the industry has transitioned to methods of detecting malware behavior to offset improvements in the capabilities of highly motivated and resourced actors to bypass blacklisting tools. As shown in Figure 2, MITRE's ATT&CK framework [MITRE 2015] identifies tactics adversaries use in the cyber attack lifecycle phases following a compromise, such as establishing persistence, moving laterally within the system, and escalating privilege. For each tactic, it comprehensively catalogs known techniques that adversaries can use to perform that tactic. For each technique, it provides a technical description, indicators, useful defensive sensor data, detection analytics, and potential mitigations.

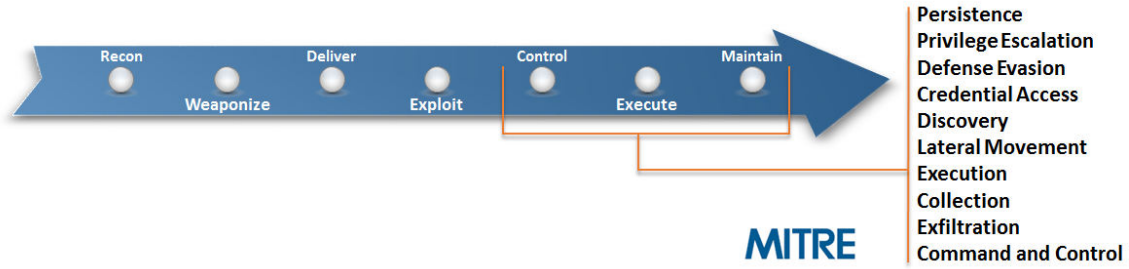

Figure 2. ATT&CK Framework Post-Compromise Adversary Tactics

This work is ongoing, and the initial release for Windows, Linux, and Mac-based endpoints and servers has been made publicly available.

Further research to develop usable detection analytics was undertaken based on the work on the ATT&CK framework, resulting in a repository of pseudocode called the Cyber Analytics Repository (CAR). (See Section 3.7.1.)

The use of an ontology of analytic elements and product-specific detection routines facilitates post-attack detection and response to minimize data exfiltration and operational impact. Consideration should also be given to development of a code repository with sector-based development and refinement to provide rapid enhancement to security operations and include support for:

- correlation of event components (multi-analytic)
- confidence-level measures to drive analytic situational understanding

- feeding response action playbook scenario selection
- refinement and updates as threats evolve

5.1.7 Resiliency Response Actions Playbook

The use and refinement of autonomous selection of possible response actions are desired outcomes of wargaming events. These COAs can be expanded and refined over time, and when coordinated with situational analytics development, can substantially reduce the impact of an event by improving response times.

Using a subset of DoD-sponsored research work, and a defined ontology for autonomous and analyst-directed COA deployment, a continuous cycle of testing and production improvements can be refined as a result of composite wargaming activity. An example of events and actions is depicted in Appendix B.

Through correlation of analytics with COA and impact awareness, events can be mapped against a set of deployed capabilities as part of the wargaming exercise to determine the severity of disruption to business operations.

5.2 Wargaming Platform Requirements

The following sections outline the requirements of a cyber wargaming platform to support scenario execution, scoring, and automation of game play.

5.2.1 Orchestration

Previous survey efforts uncovered many platforms that have been used to support wargaming efforts. Among them, the DECIDE system (see Section 3.2.1), developed by NUARI, provides a reasonable tabletop scenario builder with operator-initiated effects steps. For orchestration of attacks to actual technology platforms, the CALDERA automation system (see Section 3.2.5) provides a basis for repeatable and consistent testing of product and analytics effectiveness.

While no single known platform supports full composite (e.g., technical attack and tabletop) integration, consideration should be given to the use of these systems as a basis for further development.

5.2.2 Measures and Metrics

Incorporating a computational scoring engine into the cyber wargaming process should also be part of ongoing development efforts. This should provide the outcome of the applied effects, the impact to each individual participant's operations, and a measure of the outcome of selected COAs.

To provide more realistic results from wargaming exercises, other considerations could be included to measure the ability of the participant organizations to adapt to the attack event while maintaining ongoing availability of their critical operations. Operational elements associated with SOCs and other response organizational units could include:

- Health and welfare – ability to continue to monitor and support non-affected tasks to retain availability and acceptable performance levels.
- Support / BAU tasking – administrative changes, reporting, and external help requests
- Effects obtained and successful responses – measures of timeliness and effectiveness of response actions and choices.
- Situational awareness and event detections – time-to-live of breaches: how quickly detected, and how accurate a situational understanding of event context is achieved.

6 Composite Cyber Wargaming Scenarios

A key aspect of composite cyber wargaming exercises is the design and implementation of a believable scenario that paints the picture of the real-world event that the activity is meant to simulate. This section explains the process for achieving this and provides an extensive example. As is true throughout this report, the FSS is used as a template, but the process can be applied to any sector or industry.

6.1 Developing Wargaming Scenarios and Gaming Strategy

As previously discussed, there appears to be a gap between the type of detailed, emulation-based attacker-vs.-defender exercises conducted by the technical cyber community in test ranges and the high-level tabletop exercises conducted in the FSS (such as the Hamilton series and Quantum Dawn) to explore organizational responses and coordination in the case of major cyber events. Modeling and simulation approaches, perhaps in conjunction with testbed-based assessments and emulation, could be used to support more complex wargaming exercises that could explore the effects of variations and improvements in cyber technologies.

As an approach for enhancing wargaming of cyber risks and capabilities in the FSS or other industries, the following steps could be taken.

- Preparation
  - Develop a set of goals that could be used to define gaming objectives for a composite wargame that are not already addressed in existing cyber wargames.
  - Determine the objectives for the wargame and organizational levels of desired participants.
  - Prepare a scenario that will enable meeting the gaming objectives for a given exercise.
  - Identify a full set of requirements for a platform for the composite wargame with integration of simulation for both technical and process interaction.
- Research
  - Collect additional information regarding scenarios, exercise structure, and sector environment used to examine technology within a wargaming context in the FSS.
  - Review wargaming approaches and techniques developed in other domains, such as the DoD, for representing and exercising cyber technologies in greater detail.
  - Investigate wargaming platforms and/or simulations available in academia, industry, or government that could be adapted for FSS cyber technology-oriented wargames.
- Scope Definition
  - Analyze what level of detail (fidelity) could be achieved; what data, integration, and development effort would be required to do so; and what value it would provide in answering questions about sector or subsector cyber defense.

  - Determine the nature and characteristics of a threat model or family of threat models required to support modeling of adversary capabilities and derivation of useful scenarios for this type of wargaming.

- Exercise Design
  - Based upon research, select an initial platform or identify the components needed to build the platform for conducting the composite wargame.
    - Include increasingly sophisticated levels based on composite definitions of "crawl", "walk", and "run" [Kick 2014] to drive progression in the depth of exercise complexity.
  - Select the set of cyber technologies to be exercised, FSS institutions to be represented, business functions to be emulated or modeled, and the general nature of scenarios.
  - Prepare a completed design specification of the environment and the execution of the game to be conducted.
- Implementation
  - Assemble, adapt, and populate the threat models, using them to develop reusable adversary information and attack scenarios.
  - Assess the initial wargame plan for benefits and limitations, and use insights gained to inform development of a phased strategy for sector cyber technology wargaming.
  - Build the environment or facility specified in the design phase.
- Execution
  - Execute initial composite scenarios using a limited set of participants with a longer-term objective of building on successes towards an ultimate goal of engaging and exercising the broader sector to further identify cross-sector vulnerabilities and risk.
  - Build on infrastructure to improve simulations and technologies to bring higher fidelity to the exercise.
  - Work toward longer term objectives of:
    - Establishing a reusable testbed platform with existing threat vectors, current tools, and known results from testing and technology innovation efforts.
    - Creating a reusable game-play platform that allows for technology component reuse in the model of the National Cyber Range described in Section 3.3.2.
    - Using the testbed to test new technologies and ideas against discovered gaps in attack vector mitigation and post-compromise analytic development to improve defensive capabilities.

- Review
  - Examine the results of the wargame and assess whether the goals and objectives were met.
  - Compile lessons learned from event scenarios to improve the process for future wargame exercises
  - Assess gaps in the technology or methods
  - Identify means to reduce cost and effort for future games

The result of this approach would be a phased strategy for cyber wargaming that is focused on the secure operation and defense of cyber technology within the sector, across institutions. The phased strategy should consider the role of successive levels of tabletop, composite, and red-team wargaming. Eventually, it may be valuable to explore how live offense-on-defense adversarial play in a testbed could be incorporated as a system-in-the-loop node within a broader simulation, to enable the operation of specific cyber technologies or defenses to be studied in greater detail.

An initial discussion of cyber wargaming approaches and initial survey of cyber wargaming are presented in this report in Sections 2 and 3. The following subsections outline some considerations and directions for development and execution of composite wargames in greater detail.

6.2 Example High-Level Composite Scenario

As an approach for enhancing wargaming of cyber risks and capabilities, the merging of developed threat vector models and product evaluation mechanisms could produce additional insight into the effectiveness of deployed mitigation elements. This includes both process and technology. For example, using specific threat actor TTPs and attack vectors could provide insight into impacts against individual institutions and the overall variability of response options at the sector level when assessed against the results of various deployed cyber products' ability to address a specific vulnerability.

Most of the surveyed wargaming events focus on cyber attack and defense technology use or a process-based scenario of planning, communication, and reaction. In real-world attack events, elements of intelligence, technical response, and cross-team communication are critical to incident management efforts to contain impact, manage communications, and prevent recurrence. Outcomes from both wargaming and real-world events can be used to drive improvements in TTPs, cyber products, attribution of threat actors, and anticipation of their actions.

While there is more than one possible way to implement a composite wargaming environment, it is illustrative to examine a specific example that demonstrates how the various pieces described fit together. In this section, a hypothetical example composite wargame scenario is outlined.

6.2.1 Scenario

To demonstrate the means by which a composite wargame could be implemented, this section describes an example of "Identifying compromise of defended systems by sophisticated threat actors." This choice is warranted, given that, as stated by Symantec in [Wueest 2016], "[t]he financial sector was the most targeted sector in January 2016, with 40.2 percent of all spear-phishing attacks."[16] The report goes on to say that,

> "This underlines the high level of interest from attackers to infiltrate financial institutions and profit from the large numbers of financial transactions that flow through them.
>
> The Carbanak cybercrime group, which made headlines in February 2015, is a perfect example of a financial threat that is not just focusing on users of online banking services. This is a skilled group of attackers, capable of gaining a foothold on the networks of targeted banks through malware hidden in spear-phishing emails. Once inside, the group patiently and stealthily move across the network of a bank, gathering intelligence and compromising enough computers until it has the resources and intelligence to launch a successful attack. The Carbanak group employed two main tactics to cash out: in some cases, it transferred funds to accounts under its control; and in other instances, it compromised and hijacked ATMs in order to dispense funds to people working for the group. The exact amount stolen by the Carbanak group is unknown but estimates range from tens of millions of U.S. dollars up to $1 billion."

By modeling a scenario that follows the techniques demonstrated by the Carbanak group, a composite wargame could be developed to determine the effectiveness of various technology choices in detecting and mitigating such an advanced attack and the potential impacts on business processes of both the attack and the defenses employed.

Kaspersky appears to have been one of the first cybersecurity companies to encounter the group in the wild, and has outlined the attack cycle used by the group in a blog post[17] and in a detailed technical report [Kaspersky 2015].

Kaspersky describes the following attack lifecycle:

1. Compromise of an employee's workstation via a spear phishing email that delivers malware, establishing a command and control (C2) channel with the cybercrime group's servers on the Internet
2. Manual scanning of the targeted financial institution's internal network to identify additional machines to attack and compromise
3. Lateral movement through password harvesting and exploitation, leveraging well-known tools such as Metasploit, PsExec, and Mimikatz. Targets of the lateral movement include:

[16] According to the updated 2017 report [Wueest 2017], while this level of activity has since declined somewhat due to earlier detection, cyber attacks in the financial sector remain highly active, with large, high-profile institutions targeted and indications of involvement by nation-state actors.

[17] https://securelist.com/the-great-bank-robbery-the-carbanak-apt/68732/

a. Compromise of the workstations of employees with the ability to manipulate funds, with escalation to administrative privileges

b. Compromise of computers with access to the internal ATM network for the target financial institution

4. Execution of funds transfer using the internal assets achieved through lateral movement

a. Capture of employees' activities through video recordings that are transmitted to the cybercrime's servers for analysis and subsequent imitation.

b. Control of the ATM system from compromised system to instruct the dispenser to dump cash for pickup by a mule

6.2.2 Scenario Elements

The attack lifecycle can be used as a framework to identify technologies for foraging and testing in a composite wargame to evaluate the effectiveness of these tools at stopping such an attack scenario. Relevant technology platforms for testing in the composite wargame can be identified by mapping them to the TTPs illustrated in the attack lifecycle of Carbanak, as shown in Table 8.

Table 8. Defensive Technology Platforms Mapped to Carbanak TTPs

TTP	Network-Detect	Network-Protect	Data-Detect	Data-Protect
Spear phishing Malware delivery	Sandboxes	Email Gateway Inspection	AV / HIPS	AV / HIPS
C2 of Malware	Intrusion Detection	Next Generation Firewalls		
Lateral Movement	Intrusion Detection			
Compromise of Internal Assets			AV / HIPS	AV / HIPS
Execution of Funds Transfer			Business Processes	

Having determined the platforms to be tested, a test environment can be specified for purposes of the composite wargame event. The layers of defenses applied should be based upon what is employed in the organization conducting the exercise. After the test environment is determined, the composite wargame can be executed using the results of lab testing as a means of determining the effectiveness of each layer of defense in identifying and/or preventing a step in the hypothetical execution of the attack lifecycle. This would provide increased fidelity to determine the effectiveness of a given institution's defenses against a given composite cyber wargame scenario.

In development of wargame scenarios, the threat models described in a companion report, "Cyber Threat Modeling, Survey, Assessment, and Representative Framework" [Bodeau 2018]

will also be of considerable use. Both real-world examples and threat models should be consulted in developing scenarios.

6.2.3 Metrics

To help determine the measure of success for a defender in a given composite cyber wargaming exercise, metrics should be applied. In Section 4.2, several possible metrics were outlined for determining whether an event met its objectives or not. Where applicable, these could each be applied to the various layers of defenses implemented to understand the ability of a given FSS institution to respond to the threat actor for a given scenario.

In the scenario being considered in this example, the four suggested metrics for defenders would apply:

- Minimizing impact to business operations
- Identifying hostile activity
- Identifying exfiltration
- Remediation of compromise

Each of these would be measured through the course of the event and reviewed during the post-game activities.

6.2.4 Exercise Objectives

A primary objective of the composite cyber wargaming exercise is to accelerate adoption of IT risk-mitigating technologies by the FSS. In addition, the exercise allows institutions to test and assess vital organizational functions such as communications, IT security readiness, employee security awareness, incident response policies, and operational procedures in response to various cyber and physical incidents, to identify potential obstacles and process improvements.

The exercise aims to test an institution's preparedness for a cyber intrusion during the same time when physical attacks on dependent critical infrastructure are occurring, which can significantly hinder normal operations. By playing out each event of the scenario, the institution can assess whether and how its systems are currently protected against such an attack, and if not protected, what actions management must take to recover from the incident, prevent its recurrence, and ensure ongoing operations to minimize financial and reputational risk.

Possible environment changes can also be introduced during an exercise to help identify or validate proposed modifications to institution or sector-level processes and technology. This could also support assessment of the impact of a new vendor product or feature and determination of the value of hypothetical capability changes.

6.2.5 Wargaming Actions

Table 9 was derived from a previously published Cyber Exercise Playbook [Kick 2014] and tailored for the FSS. It depicts an orchestration flow of roughly sequential action steps to support

the exercise. This includes a context of action, details of the attack vector, potential impact from the event, and the objective of the activity.

Table 9. Wargaming Actions for Sample Scenario

ID	Title	Description	Impact	Desired Actions/Lessons Learned
1	Data Collection/ Reconnaissance	Adversaries begin data gathering/reconnaissance activities focused on the operations of a high-frequency trading firm. They search for open-source materials; perform Google searches; scrutinize company web sites for information on company officers and their social media accounts.	Attackers find extensive information in open sources (e.g., web sites, annual reports, affiliated company sites). Some officers have very active social media accounts, divulging sensitive personal information.	Company should carefully vet what types of information are publicly available and conduct routine searches for sensitive information other firms may be posting that impact the company.
2	Brute Force Attack	Attackers manage to brute force an employee's gaming account and realize the same credentials grant access to a multitude of other sites, both financial and non-financial, including access to the company's trading system.	During reconnaissance activities, attackers are tipped off by a social media post from an employee "Liking" a particular online gaming site that is relatively lax in security, allowing a brute force attack.	Employees should undergo routine training to warn about the sensitivities of posting information to social media sites and not to utilize the same username/password combinations for different sites.
3	Attack Weaponization	Adversary prepares a spear phishing email attack containing key loggers and/or malicious code which they intend to send to company employees. They are patient and wait for a prime opportunity to attack.	Attackers decide to conduct attack using spear phishing, a method with historically high success rates.	Employees should be routinely reminded about and tested for spear phishing techniques. Companies can also implement various hardware and software products to thwart phishing attacks.
4	Multiple Targets Planned	Attackers plan a separate cyber attack on a bank to steal money that will coincide with the other attacks.	Attackers take advantage of how the initial attack would cause confusion at other financial institutions as well.	Employees should be made aware that terrorists commonly deploy diversionary techniques and to always be vigilant.
5	News Monitoring	Adversaries closely monitor news sources, then see a report that a new CFO has taken over. They commence the spear phishing attack.	Attackers are very patient and are in no rush for the opportune time to attack.	The fact that there have been no terrorist attacks over extended periods of time (i.e., years, decades) does not imply that terrorists have been defeated. Terrorist organizations execute over very long time horizons.

ID	Title	Description	Impact	Desired Actions/Lessons Learned
6	Spear Phishing Exploitation	The spear phishing attack preys on the hunch that the transition to the new CFO has not been very smooth. The attackers sent spoof emails to employees in the payment operations function appearing to be from the new CFO requesting that each employee's accomplishments for the current week be sent to a new SharePoint site provided in the email. The link, however, has been spoofed to appear to be an internal web site, but the link actually deploys malware (key logger) to the system. Employees are persuaded to act quickly as the email indicates a response is required by COB today.	Attackers aim to catch employees off guard when their security attention may be diminished due to anxiety with a new CFO. Employees are not yet familiar with the new boss's work style, so receiving direct instructions from the CFO may not be unusual. Plus, the employees certainly want to appear eager and receptive to the new CFO. Although many employees may spot the spoof, only one employee needs to click on the malicious link for attack success.	Network spam filters should be up to date, ready to block malicious emails and not provide employees the opportunity to aid in the attack. Other protective measures include implementing sandboxes, email gateway inspection and antivirus/host intrusion prevention systems.
7	Installation	Key loggers/malware are successfully installed onto systems. Attackers can now download user access credentials, historical funds transfer logs, customer information, funds transfer data files, etc.	Attackers secretly lurk inside the network gathering additional information until the real attack commences.	Continuously monitor network for malicious code. Implement hardware/software solutions such as intrusion detection systems and next generation firewalls to detect malware on the system
8	Weaponization/ Exploitation/ Installation #2	Using the same data gathering and spear phishing techniques, the attackers gain access to the bank's CHIPS funds transfer system.	Attackers can now modify legitimate funds transfer instructions and/or create fake ones.	Sensitive functions such as funds transfers should require a minimum of two-party authentication, making compromise exponentially more difficult.
9	Command & Control	Malware opens a command channel to enable adversary to remotely manipulate the system. With this access, attackers prepare files to inject numerous sell orders worth billions of dollars into the company's trading systems on command.	At this point, attackers have gained access but have not yet flooded system with fake orders.	Continuously monitor network for malicious code. Implement hardware/software solutions such as intrusion detection systems and next generation firewalls to detect malware on the system
10	Physical Attack Element	The attackers decide that a multi-pronged coordinated attack will increase the magnitude and probability of	Adding a physical attack element to the primary cyber attack will cause	Terrorist organizations thrive on instilling public fear and strategically use it to promote their

ID	Title	Description	Impact	Desired Actions/Lessons Learned
		success and plan a series of simultaneous physical attacks.	greater public confusion and fear.	agenda and encourage new recruits.
11	Attacks Commence	With all plans and procedures in place, the attack commences at an opportune time.	Combination of physical and cyber attacks causes public to become paralyzed as to what is going to happen next.	Employees will tend to be distracted watching the news and not focusing on protecting systems or spotting other malicious activities.
12	Physical Attack	During morning rush hour, attackers deploy teams to local subway and Verizon buildings to commence an IED attack.	The subway attack will hinder essential employees from getting to their offices, while the attacks on Verizon buildings cause telecom degradation.	Companies should have backup transportation plans available particularly for essential employees. Contingency overnight accommodations should also be available in advance.
13	Cyber Attack	After trading opens, attackers inject numerous sell orders worth billions of dollars into the hacked company's trading systems.	Markets begin to drop precipitously, causing market circuit breakers to kick in.	Sensitive functions should require a minimum of two-party authentication, making compromise exponentially more difficult.
14	Attack Diversion	Expecting that other bank employees will notice the irregularities, the attackers also plan to divert attention from the malicious activity by flooding email system with bogus, spoofed messages coming from the new CFO stating that remedial efforts are being taken and that employees should not take any other action for the time being.	Employees do not realize that the emails from the CFO are spoofed and part of the attacker's plan.	Network spam filters should be up to date, ready to block malicious emails and not provide employees the opportunity to aid in the attack. Other protective measures include implementing sandboxes, email gateway inspection and antivirus/host intrusion prevention systems.
15	Malicious File Modification	Attackers alter recipient information of outgoing funds transfer transactions at the compromised bank and modify the MAC to accommodate the change. Funds will now be sent to a rogue account at a foreign bank.	Attackers successfully steal millions of dollars through CHIP funds transfers.	Sensitive functions should require a minimum of two-party authentication, making compromise exponentially more difficult.
16	Exploitation #3	Compounding the physical attacks on telecom and transportation, an employee of a major securities clearing firm is tricked into clicking on a malicious link in a spoofed	A successful attack against a clearing firm causes widespread anxiety as to whether trades will settle and how markets will open the following day.	Network spam filters should be up to date, ready to block malicious emails and not provide employees the opportunity to aid in the

ID	Title	Description	Impact	Desired Actions/Lessons Learned
		email, introducing malware into the clearing and settlement systems. While one single problem may not have been sufficient to cause end-of-day settlement problems, the combination of the three problems does cause an inability to clear trades for that day. Numerous corporate clients begin contacting the clearing firm asking why transactions weren't being processed.		attack. Other protective measures include implementing sandboxes, email gateway inspection and antivirus/host intrusion prevention systems.
17	Actions on Objectives	The attackers accomplish the mission's goals including instilling public fear, attacking the economy, and stealing funds.	Attackers celebrate their well-planned and successful attack.	Stopping adversaries at any stage of the attack breaks the chain and reduces the likelihood of a successful attack.

6.2.6 Exercise Participants

Typically, a tabletop exercise is geared towards assessing high-level executive, organizational response and decision making, while a red-team exercise focuses on detailed technical aspects of cybersecurity, recognizing and countering exploits, purging attackers, and identifying capability and technology gaps. Since a composite approach combines the two, participation from all levels of the organization including executive, mid- and working levels is required. The exercise incorporates both physical and cyber attacks, requiring action and coordination among technical cyber and physical security, as well as business operational functional areas.

Table 10 provides a sample (but not exhaustive) list of functional areas from which representatives are required to participate in the exercise.

Table 10. Exercise Participants

Functional Area	Responsibility
Executive Management	Provides strategic decisions impacting the long-term welfare of the company
Mid-Level Management	Supports working and executive level management and decision making
Working-Level Management	Provides day-to-day direction, decision making and organization to operational staff
Business Operational Staff (Trading, Funds Transfer, Treasury Management)	Executes steps necessary to perform business operations for the company
Physical Security	Ensures safety and integrity of the company's hard assets including buildings and employees

Functional Area	Responsibility
Security Operations Center	Monitors and secures corporate network against cyber risks, intrusions and vulnerabilities to ensure security of the company's information assets
Network Operations Center	Ensures quality of network services by performing operational monitoring of infrastructure and services. Identifies, investigates, prioritizes and escalates/resolves issues that impact network performance or availability
IT Technical Staff	Supports day-to-day network functionality, IT Help Desk and other IT-related tasks
Information Sharing and Analysis Center - FS-ISAC	Event notification across participants, analysis of events and dissemination of intelligence to participants,

7 Summary and Conclusions

Wargaming was originally developed in the context of military operations as a way of simulating an adversarial engagement that allowed for testing different scenarios of attack and response to validate designed military capabilities. It has subsequently been adapted to other operational areas, including cyber. Wargaming for cyber has been used by the DoD, DHS, technology providers, and private interests as a means of providing learning, testing processes and technology, and identifying gaps in achieving good security controls. Wargaming, both tabletop and red teaming, has proven to be a useful process for helping to advance the effectiveness of security and control in many operational settings.

Tabletop exercises have included cross-team communication, incident response, intelligence gathering and distribution, and management response scenarios. These have effectively served as a means of identifying gaps in processes and technology, and as learning exercises for administrative actions.

Red teaming, penetration testing, and capture-the-flag exercises have included both offensive, defensive, and adversarial wargaming techniques in scenario and non-scenario based events. These have also provided effective assessments of vulnerabilities in technology and process.

This work has identified next steps to develop more realistic exercises that will combine elements of the two methodologies into a composite framework that can be used not only to meet the existing cyber wargaming goals, but also to provide insight into a set of gaps and outcomes that more accurately depict normal business operations.

The following sections outline the benefits, weaknesses, and other areas that are not addressed by this cyber wargaming activity**.**

7.1 Composite Cyber Wargaming Strengths

Developing and conducting a cyber wargaming exercise allows organizations to practice their attack and response capabilities while exercising and examining human performance and decision-making in a controlled environment. Cyber wargaming has a number of advantages. Some of the more notable strengths are:

- Wargaming has a long, well-established history of use in military and government planning, assessment, and training. Cyber wargaming identifies and can be used to validate innovative cyber defense technologies that have the potential to improve cybersecurity and reduce risk from cyber sources.
- Composite wargaming in particular can provide added value. It is conducted at an intermediate level of detail between tabletop and red-team exercises, so as to efficiently balance time commitment and realism, and focuses on bridging gaps between cyber technologies and business function implications. While the two traditional types of cyber wargaming – tabletop and red teaming – are well established, creating a middle-tier that combines the two extremes promises to yield additional benefits to the advantage of the entire sector. By creating a composite exercise that borrows from both realms, additional

insight can be gleaned regarding technology capabilities or gaps and inherent cyber risks in engineering and architectural choices, without the extreme cost and effort of conducting detailed technical experiments.

- Conducting composite exercises will help achieve the goals of: (1) increasing FSS-wide situational understanding of evolving IT security risk and the technology associated with that risk; (2) improving the ability to understand and link compromises in the underlying cyber infrastructure to sub-sector operations; (3) enabling greater information flows across sub-sectors; and (4) enabling institutions to detect and neutralize adversaries more quickly and effectively than is possible today.
- Developing a cyber wargaming exercise encourages exercise planners to develop cyber risk metrics to measure success of achieving pre-defined objectives. This provides several benefits, including identifying and scoping areas needing improvement on the part of the participants, determining the effectiveness of technology in the defense presented, and identifying opportunities for improving future composite exercises.
- New technology products implemented during cyber wargaming exercises can be evaluated as to how well they protect against known gaps. Products that provide effective coverage against gaps can be considered for further evaluation.

Although this assessment is focused on the FSS, the composite wargaming exercise framework is reusable by other critical infrastructure sectors as well. In addition, it is easily adaptable; totally new exercises can be developed simply by changing the scenario, creating virtually unlimited additional learning opportunities.

7.2 Composite Cyber Wargaming Limitations

Composite cyber wargaming offers improved business operations simulation; however, some limitations to effectiveness can remain. Unknown attack vectors, unidentified vulnerabilities, and unanticipated reactions will potentially still develop. In addition, operational TTPs can change over time and affect, either negatively or positively, the ability of an institution to adapt and react.

These drive a requirement that cyber wargaming scenarios be updated and adjusted to adapt, and that a program of continuous review of cyber incidents be used to inform defenses and identify decreases in mitigation effectiveness. Finally, cyber wargaming cannot address the broader nation-state and less resource-constrained entities (e.g., terrorists, state sponsored groups) that may overwhelm an institution's business execution capacity, requiring sector-level or national intervention.

7.3 Changing Threats and Emerging Technologies

While an exercise may not help defend against emerging techniques and technologies, the use of the process model to support "what if" scenarios for forward-leaning views of changing technologies and potential attack vectors can be useful. It could then be coupled with a red team exercise to validate results.

All emerging technologies share five key attributes as defined in [Rotolo, 2015]: (1) radical novelty, (2) relatively fast growth, (3) coherence, (4) prominent impact, and (5) uncertainty and ambiguity. The use of cyber intelligence sources and analytics of actual events to reassess the effectiveness of products and processes in mitigating attacks serves as an augmentation to the continual defend-and-adapt process of cyber operations.

Processes to identify emerging technologies and to consider and test their potential for bypassing or avoiding currently deployed technologies should be used to augment cyber wargaming. The use of both sector and technology industry views for disruptive trends (such as the World Economic Forum yearly assessment of the top ten items [Cann 2016]) should be used as a basis to drive action updates and inform assessments of changes to inherent risk levels against technology mitigation, process mitigation, and business function impacts.

Appendix A Planning, Conducting, and Assessing a Composite Cyber Wargame

As identified in [Kick, 2014], to ensure a successful exercise, sufficient planning should begin well in advance. Typically, a composite cyber wargaming exercise requires at least several weeks of planning beginning several months before the exercise commences. Planning and coordinating an exercise takes a significant amount of time, especially if the exercise includes multiple entities or scenarios. The following describes the initial, mid-term, and final planning meetings typically required, as well as the types of information needed and decisions to be determined at each stage.

The first stage of planning consists of a Concept Development Meeting (CDM), which should take place anywhere between 2 to 12 months prior to the actual exercise. Topics to discuss during the CDM include objectives; internal and external participants; scenarios; logistics; and resources. In addition, planners should identify all systems applications impacting the processes to be tested during the exercise including business applications; systems that support those applications; dependent network infrastructure; and third-party application dependencies so that appropriate scenarios can be incorporated against these systems.

About 2 to 8 weeks after the CDM, planners should conduct an initial planning meeting (IPM) to review all of the work accomplished in the CDM, including the exercise scenario and objectives to ensure mutual agreement.

Exercise organizers may need to hold a Master Scenario Event List (MSEL) planning meeting after the IPM to clearly define all of the injected events needed to support the exercise scenario. Participants will work through the technical and non-technical details of drafting all injects – "real" or scripted – that support the exercise scenario.

A mid-term planning meeting should take place 2 to 8 weeks after the IPM to review the scenario, resolve action items from the previous meetings, review the rules of engagement, and review the draft MSELs to ensure all planners have a mutual understanding of the exercise. The group should also finalize the objectives and the scenario to identify any additional logistical or training requirements for the exercise.

At the final planning meeting, which should take place about one month prior to the exercise, planners should finalize any remaining details of the exercise, review previously discussed items such as the scenario, rules of engagement, MSELs, and logistics, and finalize all remaining details for the execution of the exercise.

A more detailed outline of the steps required to plan and prepare for a successful exercise includes:

1. Wargame Scope
    a. Determine how many scenarios to incorporate into the game
        i. Target number of scenarios per exercise: 2-4. Too many scenarios may dilute effectiveness and complicate planning

b. Decide how sophisticated exercises will be
    i. Could be based on technical expertise of participants
    ii. Could be based on current threat environment
c. Determine how much participation will be required
    i. What level/quantity of managerial staff participation
    ii. What level/quantity of operational staff participation
    iii. What level/quantity of technical staff participation
d. Determine what other (third-party) organizations to include
    i. Third-party suppliers
    ii. Operations contractors
    iii. Support/administrative contractors

2. Application Inventory
    a. Business applications
    b. Systems that support those applications
    c. Dependent network infrastructure
    d. Third-party dependencies
3. Concept Development
    a. Concept Development Meeting
        i. Identify wargame objectives
            1. To develop a wargame scenario reflecting current threats
            2. To exercise participant responses
            3. To assess effectiveness of cross-departmental coordination and communication
            4. To define and clarify the roles and responsibilities of cyber responders
            5. To understand decision-making authority
            6. To highlight interactions with third-party business partners
            7. To identify potential gaps in an organization's preparedness contingency and response plans.
            8. To identify potential gaps in an organization's technology threat vector mitigation.
            9. To assess ability to address an in-depth or prolonged attack

10. To test response agility to escalating crises and challenge processes and decision-makers
11. To examine how business continuity plans are enacted and adapted, identifying factors that lead to failure
12. To identify multiple points of failure, whether tactical, operational, or doctrinal

ii. Determine exercise style, scenarios, possible locations, and resources

iii. Review lessons learned from prior exercise(s)

iv. Generate scenario ideas based on objectives/scope/applications affected

v. Develop scenarios/MSELs for the exercise

1. Card injections
2. Automated injections
3. Live injections
4. Business as Usual tasks

4. Initial Planning Meeting
    a. Finalize exercise objectives
    b. Define exercise scenario
    c. Discuss preliminary rules of engagement
    d. Discuss scoring / measures of success
    e. Determine dates for the follow-up planning sessions and exercise execution
    f. Develop preliminary logistics plan (exercise location, lodging, transportation, physical security, etc.)
5. MSEL Planning Meeting
    a. Define all of the injects needed to support the exercise scenario
    b. Work through technical and non-technical details of drafting all of the injects – "real" or scripted – that support the exercise scenario
    c. Outline a series of injects that will drive the objectives of the exercise but not overwhelm the training audience
6. Mid-Term Planning Meeting
    a. Finalize exercise scenario
    b. Finalize understanding of the rules of engagement

c. Draft an exercise logistics plan (suitable location, room logistics, dates, travel, physical security, transportation, accommodations, equipment shipping instructions, etc.)

d. Finalize scoring / measures of success determinants

e. Develop training materials needed for the training audience (operating environment, procedures, policies, expectations, technical training, etc.)

f. Coordinate the resources required at the exercise location (range, type of networks, diagrams, systems, etc.)

g. Finalize coordinating the logistics plan (location, lodging, transportation, physical security, etc.)

7. Final Planning Meeting
    a. Finalize exercise scenario with senior leadership approval
    b. Finalize rules of engagement, signed by appropriate leadership
    c. Finalize exercise logistics plan (location, lodging, flight plans, transportation, physical security, etc.)
    d. Finalize training materials needed for the training audience (operating environment, procedures, policies, expectations, technical training, etc.)
    e. Finalize resource plan so resources arrive at the exercise location
8. Schedule
    a. Wargaming duration (single or multi-day)
    b. Regular business hours and/or off-hours play
    c. MSEL injection flow/cadence
9. Hotwash Meeting
    a. Schedule
    b. Participants
    c. Evaluate scoring / measures of success
    d. Develop after-action report

Appendix B Example Events and Actions

Table 11 depicts a few examples of events and actions that could be used in a composite cyber wargame, as discussed in Section 5.1.2. The events are shown in the column entitled "Threat Condition Type," while the actions are listed in the "Course of Action" column. The table also provides information about the technique that could be used to bring about the event, actions or symptoms that could be observed, and the consequences to the system or users of carrying out the corrective courses of action.

Table 11. Example Events and Actions

User-defined Criticality Entity	Risk Condition Type	Threat Condition Type	Tactic	Technique	Observable Type	Observable Source	Course of Action Type	Course of Action	Acceptable Level of Performance	Consequence
Network Device	Risk of Occurrence	Compromised Network Device	N/A	N/A	Message Broadcast	Network Device	Redundancy	Remove Compromised Device from Network and Use Backup Device	Network bandwidth and response must be the same with previous device	Very slight disruption when failing over to new network device
Service (ex.)	Risk of Occurrence	Compromised Service	Execution (of exploit)	Command line	Service Logs	Service	Segmentation / Isolation	Isolate Service in Special Utility Cloud	A maximum number of requests can be accepted while service is examined	Users may not be able to access service while it is being examined
Application (ex.)	Risk of Success	Authorized use of an application (to harm performance of a service)	Privilege Escalation	DLL Injection	API Call Monitoring	Host Memory	Segmentation / Isolation	Isolate Application in Special Utility Cloud	Application and host availability is the same	A large number of users may not be able to access application while it is being examined

User-defined Criticality Entity	Risk Condition Type	Threat Condition Type	Tactic	Technique	Observable Type	Observable Source	Course of Action Type	Course of Action	Acceptable Level of Performance	Consequence
Application (ex.)	Risk of Success	Software Integrity Attack	Privilege Escalation	Exploitation of Vulnerability	Crash Report Notification	Crash Report	Redundancy	Restore Application	Application response should continue to be the same as previous	Application or performance dependent systems may get worse
Any data determined critical to an organization	Compromise of Sensitive Data	Exfiltration	Exfiltration	Automated or scripted exfiltration	Discovered manually or automated notification	Unrecognized Process or Scripts	Monitoring	Further monitor and investigate misbehaving script	Initiate secondary course of action if application performs worse than given threshold	Application or performance of dependent systems may get worse

List of Acronyms

Acronym	Definition
AMICA	Analyzing Mission Impacts of Cyber Actions
API	Application Programming Interface
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
ATT&CK™	Adversarial Tactics, Techniques, and Common Knowledge
AV	Anti-Virus
BACS	Building Access and Control Systems
BAU	Business As Usual
BCBS	Basel Committee of Banking Supervision
BYOD	Bring Your Own Device
C2	Command and Control
CAL	Cyber Attack Lifecycle
CALDERA	Cyber Adversary Language and Decision Engine for Red Team Automation
CAPEC™	Common Attack Pattern Enumeration and Classification
CAR	Cyber Analytics Repository
CBT	Computer Based Training
CDM	Concept Development Meeting
CD-ROM	Compact Disc Read-Only Memory
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CHIPS	Clearing House Interbank Payments System

Acronym	Definition
CI	Critical Infrastructure
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COA	Course of Action
COB	Close of Business
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical Systems
CS&C	DHS Office of Cybersecurity and Communications
CSAW	Cyber Security Awareness Week
CSF	(NIST) Cybersecurity Framework
CTF	Capture the Flag
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributed Denial of Service
DECIDE	Distributed Environment for Critical Infrastructure Decision-making Exercises
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLL	Dynamic-Link Library
DNS	Domain Name System
DoD	Department of Defense
DSB	Defense Science Board
DTCC	Depository Trust and Clearing Corporation
EBT	Electronic Benefits Transfer
FEMA	Federal Emergency Management Agency

Acronym	Definition
FFIEC	Federal Financial Institutions Examination Council
FFRDC	Federally Funded Research and Development Center
FMX	Fort Meade Experiment
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSS	Financial Services Sector
FSSCC	Financial Services Sector Coordinating Council
GUI	Graphical User Interface
HIPS	Host Intrusion Prevention System
HSSEDI	Homeland Security Systems Engineering & Development Institute
IBM	International Business Machines
iCTF	International Capture The Flag
IdAM	Identity and Access Management
IED	Improvised Explosive Device
IEEE	Institute for Electrical and Electronics Engineers
IIS	Internet Information Services
IOC	Indicator of Compromise
IP	Internet Protocol
IPM	Initial Planning Meeting
ISACA	Information Systems Audit and Control Association
IS	Information Security
IT	Information Technology
LAN	Local Area Network
LARIAT	Lincoln Adaptable Real-time Information Assurance Testbed
LEO	Law Enforcement Officer

Acronym	Definition
M&A	Merger and Acquisition
M&S	Modeling and Simulation
MAC	Message Authentication Code
MIT	Massachusetts Institute of Technology
MSEL	Master Scenario Event List
N/A	Not Applicable
NCR	National Cyber Range
NGCI	Next Generation Cyber Infrastructure
NIST	National Institute of Standards and Technology
NSCSAR	NIPRNET/SIPRNET Cyber Security Architecture Review
NUARI	Norwich University Applied Research Institutes
NYSE	New York Stock Exchange
OASIS	Organization for the Advancement of Structured Information Standards
OCC	Office of Comptroller of Currency
OMG	Object Management Group
OWASP	Open Web Application Security Project
PC	Personal Computer
PDA	Personal Digital Assistant
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PMO	Program Management Office
PMP	Project Management Plan
QA	Quality Assurance

Acronym	Definition
R&D	Research and Development
RDP	Remote Desktop Protocol
RMF	Risk Management Framework
ROI	Return on Investment
S&T	Science and Technology Directorate
SA	Situational Awareness
SANS	System and Network Security
SEI	Software Engineering Institute
SIMEX	Simulation Experiment
SOC	Security Operations Center
STIX	Structured Threat Information eXpression
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAL	Threat Agent Library
TAXII	Trusted Automated eXchange of Indicator Information
TTP	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise
UCSB	University of California, Santa Barbara
USB	Universal Service Bus
VM	Virtual Machine
VPN	Virtual Private Network
WASC	Web Application Security Consortium

List of References

1. Applebaum, A., et al. 2016. "Intelligent, automated red team emulation," Proceedings of the Annual Computer Security Applications Conference, December 2016.

2. Barnum, S. 2014. "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)," Version 1.1, Revision 1, February 20, 2014. http://stixproject.github.io/getting-started/whitepaper/

3. Bodeau, D., and Graubart, R. 2011. "Cyber Resiliency Engineering Framework," MTR 110237, PR 11-4436, The MITRE Corporation, 2011. https://www.mitre.org/sites/default/files/pdf/11_4436.pdf

4. Bodeau, D., and Graubart, R. 2013. "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment," MTR 13432, PR 13-4173, The MITRE Corporation, 2013. https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

5. Bodeau, D., et al. 2018. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," HSSEDI, The Mitre Corporation, April, 2018.

6. Cann, O. June 2016. World Economic Forum, Geneva Switzerland. "These are the top 10 emerging technologies of 2016," https://www.weforum.org/agenda/2016/06/top-10-emerging-technologies-2016

7. Cloppert, M. "Security Intelligence: Attacking the Kill Chain," 14 October 2009. Available at http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain/

8. Cloud Security Alliance (CSA). 2013. "The Notorious Nine: Cloud Computing Top Threats in 2013." June 16, 2013. https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

9. Committee on National Security Systems (CNSS). 2015. "Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009," April 26, 2015. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

10. Deloitte. 2014. "An introduction to cyber war games," CIO Journal, September 22, 2014. http://deloitte.wsj.com/cio/2014/09/22/an-introduction-to-cyber-war-games/

11. Dinsmore, P. 2016, "NIPRNET/SIPRNET Cyber Security Architecture Review," AFCEA Defensive Cyber Operations Symposium, April 2016.

12. Defense Science Board (DSB). 2013. "Task Force Report: Resilient Military Systems." January 2013. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

13. Federal Financial Institutions Examination Council (FFIEC). 2016. "IT Examination Handbook for Information Security," http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf

14. Fernandes, D.A.B., Soares, L.F.B., Gomes, J.V., Freire, M.M., and Inácio, P.R.M. 2014. "Security Issues in Cloud Environments: A Survey." International Journal of Information Security 13: 113.

15. Fox, D.B. 2016. "Financial Institution Threat Library," unpublished manuscript, 2016.

16. Fox-IT. 2016. "Financial Sector and the Evolving Threat Landscape: Live Cyber Exercise," RSA Conference Learning Labs. 2016. https://www.rsaconference.com/writable/presentations/file_upload/lab1-w13_financial_sector_and_the_evolving_threat_landscape_live_cyber-exercise_-_follow_up.pdf

17. Franz, M.D. 2005. threatmind.sourceforge.net, last updated November 2005 (no longer accessible).

18. Gilad, Benjamin, 2009, *Business War Games: How Large, Small, and New Companies Can Vastly Improve Their Strategies and Outmaneuver the Competition*, The Career Press, Inc.

19. Hutchins, E.M., Cloppert, M.J., and Amin, R.M.l. 2010. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceedings of the 6th International Conference on Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113–125; https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

20. Imperva. 2015. "Man-in-the-Cloud (MITC) Attacks." September 22, 2015. https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

21. Intel. 2007. "Threat Agent Library Helps Identify Information Security Risks." September 2007. https://communities.intel.com/docs/DOC-23853

22. Intel. 2015. "Understanding Cyberthreat Motivations to Improve Defense," February 13, 2015. https://communities.intel.com/servlet/JiveServlet/previewBody/23856-102-1-28290/understanding-cyberthreat-motivations-to-improve-defense-paper-l.pdf

23. Kaspersky. 2015. "Carbanak APT, The Great Bank Robbery," Kaspersky Lab, February 2015. https://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf

24. Kemmerer, M. 2016. "Detecting the Adversary Post-compromise with Threat Models and Behavioral Analytics," 7th Annual Splunk Worldwide Users' Conference, 2016. https://conf.splunk.com/files/2016/slides/detecting-the-adversary-post-compromise-with-threat-models-and-behavioral-analytics.pdf

25. Kick, J. 2014. "Cyber Exercise Playbook," MP140714, The MITRE Corporation, November 2014. https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

26. Kordy, B., Piètre-Cambacédès, L., and Schweitzer, P. 2014. "DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Trees," Computer Science Review, Volume 13, Issue C, pp. 1-38. November 2014.

27. Lockheed Martin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

28. McCombie, S., et al. 2016. "Cyber-Monkey 2016, Learning Lab Summary," RSA Conference Learning Labs. 2016. https://www.rsaconference.com/writable/presentations/file_upload/lab-r02_cyber-wargame_exercise_operation_cyber-monkey_2016_-_follow_up.pdf

29. The MITRE Corporation. 2009. "One Step Ahead: MITRE's Simulation Experiments Address Irregular Warfare," September 2009. https://www.mitre.org/publications/project-stories/one-step-ahead-mitres-simulation-experiments-address-irregular-warfare

30. The MITRE Corporation. 2012. "Cyber Observable eXpression (CybOX™)," November 2012. http://cyboxproject.github.io

31. The MITRE Corporation. 2012b. "MITRE's Fort Meade eXperiment (FMX): Research in Intra-Enclave-Level Cyber Defenses," PR 12-3942, 2012.

32. The MITRE Corporation. 2012c. "Threat-Based Defense: A New Cyber Defense Playbook," July 2012. https://www.mitre.org/sites/default/files/pdf/cyber_defense_playbook.pdf.

33. The MITRE Corporation. 2015. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)," 2015. https://attack.mitre.org/wiki/Main_Page

34. The MITRE Corporation. 2016. "Common Attack Pattern Enumeration and Classification (CAPEC)," June 2016. http://capec.mitre.org

35. The MITRE Corporation. 2017. "BRAWL: Blue vs Red Agent War-game evaLuation," August 2017. https://github.com/mitre/brawl-public-game-001

36. National Cyber Range (NCR). 2015. "National Cyber Range Overview." http://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf.

37. National Institute of Standards and Technology (NIST). 2013. "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, Revision 4, April 2013.

38. National Institute of Standards and Technology (NIST). 2014. " Framework for Improving Critical Infrastructure Cybersecurity," Revision 1, February 2014.

39. Noel, S., et al. 2015. "Analyzing Mission Impacts of Cyber Actions (AMICA)," NATO IST-128 Workshop on Cyber Attack Detection, Forensics, and Attribution for Assessment of Mission Impact, Istanbul, Turkey. http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf

40. OASIS Cyber Threat Intelligence (CTI) Technical Committee. 2016. "STIX 2.0 Specification: Objects and Vocabularies, Version 2.0, Draft 1," https://www.oasis-open.org/committees/download.php/58539/STIX2.0-Draft1-Objects.pdf

41. Perla, P., et al. 2002. "Wargame-Creation Skills and the Wargame Construction Kit." https://www.cna.org/cna_files/pdf/D0007042.A3.pdf

42. Rossey, L., et al. 2002 ."LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed," Proceedings of the IEEE Aerospace Conference, 2002.

43. SecureWorks. 2016. "Advanced Persistent Threats: Learn the ABCs of APTs - Part A," September 27, 2016. https://www.secureworks.com/blog/advanced-persistent-threats-apt-a

44. Steiger, S. 2016. "Maelstrom: Are you playing with a full deck? Using an Attack Lifecycle Game to Educate, Demonstrate and Evangelize," 2016. https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Shane-Steiger-Maelstrom-Are-You-Playing-With-A-Full-Deck-V14-Back.pdf

45. Strom, B., et al. 2017. "Finding Cyber Threats with ATT&CK™-Based Analytics," MTR 170202, PR 16-3713, The MITRE Corporation, June 2017.

46. Temin, A., and Musman, S. 2010. "A Language for Capturing Cyber Impact Effects," MTR 100344, PR 10-3793, The MITRE Corporation, 2010.

47. UcedaVelez, T. and Morana, M.M. 2015. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*. May 2015. John Wiley & Sons, Inc.

48. Wueest, C. 2016. "Symantec Security Response, Financial Threats 2015," Symantec, March 22, 2016. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/financial-threats-15-en.pdf

49. Wueest, C. 2017. "Internet Security Threats Report (ISTR) Financial Threats Review 2017, an ISTR Special Report," Symantec, May 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf